

Employers and Homeland Security: The United States' Strategy for Combating Terrorism and its Direct Impact on Employers

by Zulima V. Farber and Khizar A. Sheikh

The events of Sept. 11, 2001, and subsequent federal and state efforts to combat terrorism and crime, have increased exponentially the duties and responsibilities of employers of all sizes and in all industries, as they are called upon to assist in preventing future terrorist attacks. Principally, that assistance revolves around the government's efforts to limit the flow of people from and money to terrorist and criminal groups. But the new and increased duties and responsibilities placed on employers in this regard go much further.

Employers have longstanding obligations to safeguard their employees' privacy, and to provide discrimination- and harassment-free, safe workplaces for every employee. However, now more than ever, employers, their human resources staff, and their attorneys will have to be extra vigilant in monitoring legislative and regulatory activity, and be prepared to implement new policies and procedures to adapt quickly to the changing employment landscape, as circumstances and anti-terrorism procedures and related technologies advance.

The federal government's overall plan and objectives to fight terrorism are set forth in a document titled The National Strategy for Combating Terrorism. That plan, which became effective in Sept. 2006, is premised on the fact that, like all governments, the United States has "no higher obligation than to protect the lives and livelihoods of its citizens."¹ The National Strategy consists of several action items that, implemented in concert, will help the government protect its citizens from the threat of terrorism. Three of those action items are of particular interest to employers because they require their participation in implementation. Those three are:

1. attacking terrorists and their capacity to operate;
2. denying terrorists entry to the United States and disrupting their travel internationally; and
3. defending potential targets of attack.²

This article discusses the impact these post-Sept. 11 requirements have had on employers, and offers recommendations intended to make employers' compliance easier and less costly, and to minimize employers' risks of noncompliance.

Attacking Terrorists and Their Capacity to Operate

In devising the National Strategy, the government looked closely at the evidence showing that terrorists and criminals use our financial systems to transfer money and secure various forms of material support necessary for the operation and survival of terrorist organizations.³ Not surprisingly, to hide their activities, terrorist organizations and criminals launder money through, and use, legitimate businesses and financial institutions. So, a part of the National Strategy is directed at making it difficult or nearly impossible for terrorists to engage in money laundering or criminal financing.

To be sure, the government's anti-money-laundering

efforts have been ongoing for almost 40 years. The Bank Secrecy Act of 1970 (BSA)⁴ and related legislation required insured depository institutions, and later other specified financial institutions, to maintain certain records and report certain currency transactions as a way to permit law enforcement authorities to investigate suspicious transactions.⁵

Since the events of Sept. 11, however, new laws and regulations have been enacted that have significantly broadened the number and types of companies falling within the definition of “financial institution,” and thus requiring compliance with anti-money-laundering procedures. For example, just weeks after Sept. 11, 2001, on Oct. 26, Congress enacted the USA Patriot Act,⁶ which, at Title III, amends the BSA to require financial institutions to adopt and implement internal anti-money-laundering policies and procedures that comply with specific rules issued by, among others, the Securities and Exchange Commission and the Treasury Department. In addition, the act requires many of these financial institutions to verify the identity of those with whom they do business, and of those with whom they enter into financial transactions, and to be able to recognize “red-flags” that trigger the required filing of suspicious activity reports (SARs).⁷

Not only did the USA Patriot Act expand and toughen anti-money-laundering policies, but it also expanded the types of institutions covered. In the past, anti-money-laundering laws and regulations had defined “financial institutions” to include certain specified businesses. But the definitions of “financial institutions” and “suspicious transactions” are not entirely specific, and much more fluid, a circumstance that may require all employers, not just those specified in the pre-Sept. 11 laws, to be cognizant of the requirements because they may well fall within the

definition and be required to comply.

For example, the USA Patriot Act extends the reach of its anti-money-laundering provisions to financial institutions that previously had not been subjected to BSA regulation, such as mutual funds, futures commission merchants, commodity trading advisors, and commodity pool operators.⁸ The reach goes even further to include “any business or agency which engages in any activity which the Secretary of the Treasury determines, by regulation, to be an activity which is similar to, related to, or a substitute for any activity in which any business described in this paragraph is authorized to engage,” and “any other business designated by the Secretary whose cash transactions have a high degree of usefulness in criminal, tax, or regulatory matters.”⁹ Further, suspicious transactions can include violations such as securities fraud.¹⁰

Arguably, then, there is a risk that any employer who deals with money transactions, and any transaction that may violate federal or state law, is subject to the USA Patriot Act’s anti-money-laundering provisions. (New Jersey’s money-laundering law is patterned after the federal law.)¹¹ Complying with these new requirements can result in changes in the very nature of a business’s practices. By way of example, consider the risk posed by an employee whose job it is to receive payment or investment funds, and who accepts funds that, in fact, turn out to be derived from terrorist or criminal activity. The challenge to the employer is to implement procedures and safeguards that minimize this risk.

Lesser known but just as important to employers as the USA Patriot Act is Executive Order 13224,¹² issued on Sept. 23, 2001. The order prohibits any U.S. person or entity, as that term is defined in the order,¹³ from entering into any transaction or conducting any business with any person or entity whose name appears on the Specially Designated

Nationals and Blocked Persons List (SDN list) of the United States Treasury Office of Foreign Assets Control (OFAC), and from participating in a transaction involving an SDN’s property or interest in property.¹⁴ Because Executive Order 13224 applies to all U.S. persons and companies, not just to financial institutions,¹⁵ it has had an immediate impact on all employers. That is because, in effect, the order requires all employers to have procedures in place that will permit them to determine whether persons or entities with whom they do business (including employees) appear on the SDN list.

The SDN list is updated frequently, so companies need the means to periodically verify that they are not transacting business with a listed party (and prove their compliance). The authors recommend, in addition to ensuring strict compliance with these requirements, that companies include in all contracts and agreements a provision by which the party or parties on the other side certify under oath that they have no ties to terrorist organizations, and are not engaged in any illegal activities. The authors caution that this practice, if adopted, must be used uniformly to avoid or minimize potential liability for violating federal or state anti-discrimination laws.

Denying Terrorists Entry to the U.S. and Disrupting Their Travel Internationally

Despite pre-Sept. 11 laws requiring foreigners to present specific forms of identification and valid visas to enter the United States,¹⁶ thousands of people enter this country each year with false or no documents. Most are otherwise law-abiding individuals looking for work and a better life for their families. But many criminals and terrorists have taken advantage of our lax border security measures, and have entered and continue to enter this country with stolen or forged identification docu-

ments.¹⁷ They then may use the fraudulent identification documents to secure jobs. That some of these unauthorized workers pose a serious homeland security threat, especially if employed at sensitive facilities—nuclear plants, chemical plants, military bases, defense facilities, airports and seaports—is self evident, and has long been a subject of concern for immigration and law enforcement officials. That concern increased dramatically after the events of Sept. 11, when the authorities discovered that terrorists use false identities, fraudulent identification documents, and fictitious Social Security numbers.¹⁸

As part of their efforts to prevent the use of forged documents and minimize future acts of terrorism, federal, state, and local governments have stepped up their enforcement efforts against employers who (unknowingly or knowingly) accept false documents from potential employees.

For over 20 years, the Immigration Reform and Control Act of 1986 (IRCA)¹⁹ has required employers to comply with an employment verification process, and has had in place a sanctions program for fining employers for non-compliance. Prior to the events of Sept. 11, the verification process consisted of an employer's review of specified documents prospective employees would have to present to prove their identity and work eligibility.²⁰ Employers would send the Social Security Administration (SSA) earnings reports (W-2) forms, which would list an employee's name and Social Security number.²¹ Also, on a Form I-9, employers would certify that they had reviewed the documents presented, that the documents appeared to be genuine and to relate to the individual who had presented them, and that the employee appeared to be eligible to work in the United States.²²

This system proved ineffective for two reasons: the use of fraudulent documents undermined the employment verification process,²³ and worksite

enforcement efforts relied on a sanction system of administrative fines that usually were so modest that some employers treated them as merely a cost of doing business.²⁴ Employers today must recognize that Sept. 11 changed all that, and that both federal and state governments have moved aggressively to address the shortcomings of the old enforcement system. They are doing so by making it more expensive for companies to employ undocumented workers (through increased liability risks), while making it easier for employers to verify the documentation and identities of potential new hires.

Before Sept. 11, the risk that an employer who violated the laws prohibiting the hiring of undocumented workers would be caught was relatively low, as the Immigration and Naturalization Service (INS), the federal agency charged with enforcing those laws, did not make this aspect of its mission a priority.²⁵ It is, therefore, little wonder that as of 2004 an estimated 12 million undocumented immigrants had entered this country,²⁶ and millions of them had entered the workforce.

The events of Sept. 11 led to a drastic change in the government's resolve to secure its borders. Congress scrapped the INS and created in its place the U.S. Immigration and Customs Enforcement Agency (ICE), and replaced the old enforcement system of administrative hearings and fines with a tough combination of criminal prosecutions and asset forfeitures. These changes have resulted in dramatic increases in the number of worksite enforcement actions, arrests and criminal prosecutions of employers who hire undocumented workers.²⁷ Moreover, these criminal enforcement actions have not been limited to federal charges for alleged violation of the immigration laws, (which carry severe penalties, including imprisonment);²⁸ they have included federal charges for harboring

illegal aliens, money laundering, and violation of the Racketeer Influenced and Corrupt Organizations Act (RICO), as well as state charges of identity theft and money laundering.²⁹

The government has not hesitated to prosecute companies for these violations based on evidence that they were aware, or should have been aware,³⁰ of immigration violations at their own or their subcontractor's worksites.³¹ This represents a significant policy change from the policy that underlied the enforcement practices over the previous two decades under IRCA.

The change has had an enormous impact on American employers. A few examples from the numerous, well-publicized more recent enforcement actions make this point clear:

- On Oct. 23, 2003, ICE conducted a series of immigration enforcement actions at 60 Wal-Mart stores in 21 states, and arrested approximately 245 undocumented aliens employed not by Wal-Mart, but by its cleaning contractors. Following the arrests, ICE and Wal-Mart entered into a civil resolution that included the payment of \$11 million to the Treasury Forfeiture Fund for the purpose of promoting ICE's future law enforcement programs and activities in this field.³² This example made crystal clear the fact that employers would not escape liability for violating immigration laws by subcontracting.
- On Feb. 22, 2007, prosecutors announced the indictment of three executives of a national cleaning company for harboring illegal aliens and evading taxes. The indictment alleges that the defendants failed to collect and pay federal income, Social Security, Medicare, and employment taxes totaling over \$18 million. The indictment further alleges the defendants had disguised the true nature of their activities and had obstructed

the IRS in the performance of its governmental functions by creating several shell companies and bank accounts to hide their excess funds. Finally, the indictment alleges that the three executives used these excess funds to pay personal expenses, and includes notice that the government will seek forfeiture of all illegal proceeds.³³ In other words, the days when employers would simply pay a small fine they could treat as the cost of doing business for violating immigration laws are over, and employers who engage in illegal hiring must be prepared to pay a high price for such violations.

- On March 2, 2007, the president of an Ohio temporary labor service was sentenced to 15 months in prison for conspiring to provide undocumented workers to a national air cargo company. In this case, the evidence showed that the SSA issued notices to the company in 2002, 2003 and 2004, listing hundreds of workers employed by the company who were using invalid Social Security numbers. Despite these notices, the company continued to employ the workers, and took no substantive action to determine whether they were authorized to work in the United States. To the 15-month prison sentence, the court added the company's forfeiture of \$12 million, and the president's forfeiture of personal real estate.³⁴ Again, employers must understand that they may be held liable for violations they should have known about through notice from the SSA or another government agency.
- On March 29, 2007, law enforcement agents executed criminal and civil search warrants, and conducted consent searches at nine temporary service companies located in the Baltimore area. ICE acted as the lead investigating agency, assisted by the Maryland State Police, Baltimore City

Police, Baltimore County Police, Anne Arundel County Police and Customs & Border Protection.³⁵ This example demonstrates the high commitment to cooperation between and among law enforcement agencies at all levels in enforcing immigration laws in the workplace, a phenomenon of post-Sept. 11 America, where before, law enforcement agencies' turf battles had been legendary.

While engaged in these targeted enforcement actions, the government also is taking steps to make it easier and faster for employers to comply with their duty to verify the identity and immigration status of potential hires. To this end, the federal government has implemented an Employment Eligibility Verification Program (EEV), formerly known as the Basic Pilot Program. Still in its early stages, EEV involves verification checks of the SSA and Department of Homeland Security (DHS) databases, using an automated system to verify the employment authorization of all newly hired employees.

An employer's participation in EEV is voluntary, and is currently free. It is reasonable to expect that, once this pilot program proves successful in helping employers verify the identity and immigration status of potential hires quickly and securely, the government will seek to require all employers to use the EEV or a similar system. In fact, the proposed Comprehensive Immigration Reform Act of 2007³⁵ includes a provision that would do just that. Although the legislative effort has stalled, it is safe to predict that, in the not-too-distant future, legislation requiring all employers to use the EEV or a similar system will become law, either as part of a wider immigration reform proposal, or on their own. It follows, then, that employers would be well-advised to begin, as soon as possible, to prepare for this eventuality by considering what changes would be

required in their own processes to use the EEV systems.

Another mechanism the government has implemented since Sept. 11 to help employers reduce their risk of liability for violating immigration laws is the IMAGE Program (ICE's Mutual Agreement Between Government and Employers Program), which was unveiled in July 2006. The program requires participating employers to join in Basic Pilot/EEV; to submit to an audit of employees' work eligibility documentation (I-9 employee verification documents); to ensure the accuracy of their wage reporting by verifying their employees' Social Security numbers; and to commit to implementation of nine "best hiring practices."³⁷

Some high-profile employers have stepped up their internal compliance and enforcement programs. In 2006, obviously to better insulate the company from potential civil and criminal liability, Dunkin' Donuts' parent company, Dunkin' Brands, began requiring all of its franchisees to participate in the Basic Pilot/EEV verification program and to perform background checks of potential hires. But the company did not stop there. This year, Dunkin' Brands has moved aggressively against non-compliant franchisees by seeking to terminate their franchise agreements for alleged violations of the "obey all laws" clause in their agreements. In New Jersey, Dunkin' Brands filed a lawsuit against a non-compliant franchisee in April 2007. Similar lawsuits have been filed in other jurisdictions. The lawsuit is at its beginning stages.³⁸ Employers would be well-advised to put a program in place to determine whether enrolling in the EEV/Basic Pilot or IMAGE program is in their best interest.

Defend Potential Targets of Attack

As the Sept. 11 attacks on the Twin Towers demonstrated, terrorists and

criminals tend to stay away from hardened sites, such as military facilities, and prefer softer targets, such as corporate worksites and other places of business where large numbers of civilians gather and that are not always well-secured.³⁹ In the face of this fact, employers, especially those with hundreds or thousands of employees in any one location, must put in place policies and procedures that protect their employees and worksites from possible damage from a terrorist attack.

The Occupational Safety and Health Act of 1970 (OSHA)⁴⁰ mandates that all employers provide safe and healthful working conditions for their employees.⁴¹ But after Sept. 11, the nature and magnitude of potential workplace hazards changed and grew to include the risk of terrorism. Therefore, all employers—not just those in certain industries—should carefully consider the advisability of adopting emergency plans and procedures to prepare for potential disasters, including possible terrorist attacks, and should implement worksite evacuation policies and other safety measures that comply with OSHA guidelines (*e.g.*, explosion planning, evacuation planning).⁴² (For some employers, those specified in OSHA and its implementing regulations, such plans and procedures have been, and still are required.)⁴³ In doing so, however, employers must take care not to run afoul of federal and state laws and regulations that protect employees' rights. For example, in devising an evacuation plan, employers must consider the special needs of disabled employees, and must reasonably accommodate those needs lest they risk violating the Americans With Disabilities Act (ADA),⁴⁴ which prohibits employers from asking employees whether they will need assistance in an emergency situation.⁴⁵

Here, too, the government has acted to assist employers in the planning and implementation of emergency plans by issuing guidance that includes how to

protect employee rights.⁴⁶ In particular, the Equal Employment Opportunity Commission (EEOC) has issued an advice memorandum that permits employers to seek certain otherwise prohibited information, if they do so: (a) with all employees after making a job offer but before employment begins, (b) as part of a voluntary, periodic survey of all current employees to determine whether they will require assistance in an emergency, or (c) only with those employees with known disabilities if they will require assistance in the event of an emergency.⁴⁷

Certain employers in the healthcare industry must additionally ensure they comply with the Health Insurance Portability and Accountability Act of 1996 (HIPAA) Privacy Rule, which protects individually identifiable health information from disclosure.⁴⁸ The U.S. Department of Health and Human Services has provided a "decision tool" to help employers determine when and to whom private, confidential information may be disclosed.⁴⁹ Employers are advised to make use of this tool as they formulate emergency plans.

To minimize the threat of recognizable workplace hazards, among other reasons, employers have traditionally been careful not to hire people who may cause harm to others. Among the best ways to screen potential employees is conducting thorough and complete background checks. While this practice is effective, it does carry the risk of violating important employee rights, including the right to privacy and to be free of discrimination and illegal harassment.⁵⁰

Employers must take special care to minimize those risks; this can be accomplished by adopting such relatively simple procedures as requiring all applicants to complete a written application and verifying education, employment history and related information (certificates, licenses, etc.). Depending on the industry and the position, applicant

screening may require more complicated and costly procedures, such as fingerprinting, obtaining a criminal history and credit report, Social Security number verification and cross-referencing against law enforcement advisories and terror watch lists.⁵¹ When performing the more-invasive types of background checks, employers must bear in mind that they are still required to comply with other applicable state and federal laws, including the federal Fair Credit Reporting Act (FCRA),⁵² which regulates the collection, dissemination, and use of consumer credit information.

The authors note that while most employers have a choice of whether and when to conduct background checks, and, if so, what type, some employers do not have that choice. For example, New Jersey's P.L.2006, c.101,⁵³ which became effective on Sept. 15, 2007, requires criminal history background checks and identity verification checks on applicants to be employed in critical positions by independent contractors within designated facilities, such as chemical plants and other industrial sites.⁵⁴ The term "designated facility" means those facilities whose owners or operators are required to submit a registration form in accordance with the Toxic Catastrophe Prevention Act,⁵⁵ and the act defines critical positions as "any title or position in which the duties or responsibilities may potentially affect the public safety or national security or in which the applicant may have access to information which may potentially affect the public safety or national security."⁵⁶

Employers should keep in mind that other laws, including state and federal privacy protection laws, may impact employers' conduct, as may the terms of any applicable collective bargaining agreement. Employers should obtain professional advice before embarking on wholesale background checks of employees and/or applicants.

One final issue relating to background

checks and employee privacy deserves special consideration. The USA Patriot Act gave enhanced investigative powers to federal and state law enforcement authorities, and changed the manner in which federal law enforcement officials may obtain certain forms of wire communication—including voicemail messages—and tangible things.⁵⁷ The act requires employers to respond and comply with certain wiretapping orders and search warrants issued pursuant to it, and not to disclose to the target employee the fact that the government has requested and obtained information relating to him or her.⁵⁸

An employer who has adopted personnel policies protecting the confidentiality of employee records should amend these policies to include notice that it must and will fully comply with all lawful requests from law enforcement authorities for employee information, including confidential employee information. As a further safeguard, employers should amend policies and procedures for responding to lawful information requests from government agencies. The adoption of such uniform policies will minimize the risk that the employer will be liable for failure to comply with law enforcement demands, or for violating employee rights in doing so.

Conclusion

The Sept. 11 terrorist attacks had profound consequences in our country that went beyond the personal and property damages that occurred that day. As all levels of government assessed the additional resources and procedures needed to prevent future terrorist attacks, they recognized that employers would, of necessity, be called upon to assist in vital ways in implementing the National Strategy. As a consequence, employers face additional, some might say onerous, burdens to comply with new laws and regulations relating to the worksite,

employees, job applicants, and third parties. Employers also face higher risks and penalties for failure to comply with the new requirements.

Recognizing the complexity and costs of the new burdens, the government has strived to help employers by implementing compliance programs and providing valuable guidance. The burdens on employers are multiplied because they also are required to comply with all applicable laws enacted to protect employees' rights.

To minimize the risks of non-compliance, employers must be particularly attentive to changes in employment laws and regulations, must make use of every available compliance tool, and must use extraordinary care in selecting the human resource and other employment professionals who will advise and guide them through the thicket of applicable and sometimes seemingly contradictory laws. By so doing, employers will be best positioned to protect their own and their employees' interests, and to balance their needs with the government's paramount duty to protect the lives and livelihoods of its citizens. This article is intended to help employers meet their varied obligations and achieve their goals in the area of homeland security. ☺

Endnotes

1. See National Strategy for Combating Terrorism, at 11 (Sept. 2006), www.whitehouse.gov/nsc/nsct/2006/.
2. See National Strategy, at 11-13, *supra*, note (1).
3. See National Strategy, at 12, *supra*, note (1).
4. The BSA is codified at 31 U.S.C.A §§ 5311 to 5330, and its implementing regulations are located at 31 C.F.R. 103.
5. Initially, regulations applying the anti-money-laundering provisions

of the BSA were issued only for banks and certain other institutions that offered bank-like services or that regularly dealt in cash. See 31 C.F.R. 103.18 to .25. In 1992, Congress added anti-money-laundering provisions to the BSA, which authorized the U.S. Treasury to apply the law to many different types of financial institutions. A Report to Congress in Accordance with § 356(c) of the USA Patriot Act, Dec. 31, 2002, (Patriot Act Report), at 2-3, *available at* www.fincen.gov/356report.pdf.

6. The full title of the USA Patriot Act is The Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism Act of 2001, (Patriot Act), Pub. L. No. 107-56, 115 Stat. 272 (2001) (codified in various sections of U.S.C.).
7. 2007 National Money Laundering Strategy, Appendix D, Status of BSA Regulations for Financial Institutions (2007), www.ice.gov/doclib/pi/financial/2007nmls.pdf.
8. 31 U.S.C.A. § 5312(a)(2); See also Patriot Act Report, at 4, *supra*, note (5).
9. *Id.*
10. A suspicious transaction can even include securities fraud. See, e.g., SEC Institutes Enforcement Action Alleging Broker-Dealer and Its Principal Aided and Abetted Pump-and-Dump Scheme and Failed to File Suspicious Activity Reports Required by Bank Secrecy Act (April 11, 2007), www.sec.gov/news/press/2007/2007-64.htm.
11. N.J.S.A. 2C:21-25 *et seq.*
12. See Executive Order 13224, 66 Fed. Reg. 49,079 (Sept. 23, 2001) (codified at 31 C.F.R. part 594), *available at* www.state.gov/s/ct/rls/fs/2002/16181.htm.
13. *Id.*, at § 3.
14. The current SDN list is available at

- www.treas.gov/offices/enforcement/ofac/sdn/.
15. See Executive Order 13224, at § 3, *supra*, note (13).
 16. See Department of Homeland Security, Crossing U.S. Borders, available at www.dhs.gov/xtrvlsec/crossing-borders/.
 17. See National Strategy, at 13, *supra*, note (1).
 18. See *Fraudulent Identification Documents and the Implications for Homeland Security*: Hearing before the H. Select Comm. on Homeland Sec., 108th Cong. (Oct. 1, 2003) (testimony of John S. Pistole, assistant director, Counterterrorism Division, FBI), available at www.fbi.gov/congress/congress03/pistole100103.htm.
 19. Pub. L. No. 99-603, 100 Stat. 3359 (1986).
 20. United States Government Accountability Office, *Preliminary Observations on Employment Verification and Worksite Enforcement Efforts* (released June 21, 2005), (GAO Worksite Report), www.gao.gov/new.items/d05822t.pdf.
 21. Safe-Harbor Procedures for Employers Who Receive a No-Match Letter, Proposed Rule, 71 Fed. Reg. 34281 (proposed June 14, 2006) (to be codified at 8 C.F.R. pt. 274a), (ICE No-Match Proposed Regulation).
 22. Department of Homeland Security, U.S. Citizenship and Immigration Services, Employment Eligibility Verification Form I-9 (Rev. 5/31/05), page 2.
 23. See GAO Worksite Report, *supra*, note (19).
 24. President Bush's Plan For Comprehensive Immigration Reform, www.whitehouse.gov/stateoftheunion/2007/initiatives/immigration.html.
 25. See GAO Worksite Report, *supra*, note (19).
 26. Pew Hispanic Center, *Size and Characteristics of the Unauthorized Migrant Population in the U.S., Estimates Based on the March 2005 Current Population Survey* (March 7, 2006), available at <http://pewhispanic.org/reports/report.php?ReportID=61#OtherTitle>.
 27. Fact Sheet: A Record of Achievement on Border Security and Worksite Enforcement, www.whitehouse.gov/news/releases/2007/05/print/20070523-2.html.
 28. 8 U.S.C.A. § 1324a(f).
 29. Fact Sheets, Worksite Enforcement (Feb. 22, 2007), www.ice.gov/pi/news/factsheets/worksite070222.htm.
 30. Even prior to Sept. 11, an employer could be in violation of Section 274A(a)(2) of IRCA, 8 U.S.C.A. 1324a(a)(2), by having constructive knowledge rather than actual knowledge that an employee was unauthorized to work. 8 C.F.R. 274a.1(l)(1). Since Sept. 11, ICE has proposed a regulation that would increase the number of situations that may lead to a finding that an employer had such constructive knowledge, including an employer's failure to take reasonable steps in response to either of two events: 1) the employer received written notice from the SSA that the combination of name and Social Security account number submitted to the SSA via W-2 Form for an employee does not match agency records; or 2) the employer receives written notice from the DHS that the immigration status or employment authorization documentation presented or referenced by the employee in completing Form I-9 was not assigned to the employee according to DHS records. See ICE No-Match Proposed Regulation, *supra*, note (20).
 31. Fact Sheet: Immigration Fact Check: Responding to Key Myths, www.whitehouse.gov/news/releases/2007/05/print/20070522.html.
 32. See ICE provides \$2.5 million to Pennsylvania law enforcement agencies for their assistance in immigration investigation of Wal-Mart and contract companies (Aug. 14, 2006), www.ice.gov/pi/news/newsreleases/articles/060814dc.htm.
 33. See Three Executives of National Cleaning Company Indicted for Harboring Illegal Aliens and Evading Taxes, Employees arrested at 63 locations in 17 states and D.C., (Feb. 22, 2007), www.ice.gov/pi/news/newsreleases/articles/070222grandrapids.htm.
 34. See President of Garcia Labor Companies sentenced to 15 months in prison for conspiring to provide illegal workers to a national air cargo firm. Companies ordered to forfeit \$12 million, the largest such forfeiture ever (March 2, 2007), www.ice.gov/pi/news/newsreleases/articles/070302CINCINNATI.htm.
 35. See ICE arrests illegal aliens in Baltimore worksite enforcement operation. Employment services firm allegedly provided Baltimore businesses with illegal aliens (March 29, 2007), www.ice.gov/pi/news/newsreleases/articles/070329baltimore.htm.
 36. S. 1348, 110th Cong. § 301 (2007).
 37. See IMAGE: ICE Mutual Agreement between Government and Employers, www.ice.gov/partners/opaimage/.
 38. 29 U.S.C.A. § 651 *et seq.*
 39. See National Strategy, at 13, *supra*, note (1).
 40. 29 U.S.C.A. § 651 *et seq.*,
 41. See *Dunkin Donuts Franchised Restaurants LLC v. Anuja, Inc., et al.*, No. 07-cv-1841 (D.N.J. April 24, 2007).
 42. See, e.g., Evacuation Planning Matrix, available at www.osha.gov/dep/evacmatrix/index.html; Fire and Explosion Planning Matrix, available at www.osha.gov/dep/fire-expmatrix/index.html.
 43. See 29 C.F.R. 1910.38 (requiring employers to have an emergency action plan "whenever an OSHA standard in this part requires one").
 44. 42 U.S.C.A. § 12101 *et seq.*

45. 42 U.S.C.A. § 12112(d).
46. 42 U.S.C.A. § 12101 *et seq.*
47. Equal Employment Opportunity Commission, Fact Sheet on Obtaining and Using Employee Medical Information as Part of Emergency Evacuation Procedures (modified Oct. 27, 2005), www.eeoc.gov/facts/evacuation.html.
48. 45 C.F.R. 164.501 *et seq.* HIPAA is codified in various sections of 18 U.S.C.A., 26 U.S.C.A., 29 U.S.C.A., and 42 U.S.C.A.
49. Department of Health and Human Services, Office for Civil Rights, HIPAA Privacy Rule: Disclosures for Emergency Preparedness—A Decision Tool, www.hhs.gov/ocr/hipaa/decision-tool/.
50. *See, e.g.*, Title VII of the Civil Rights Act of 1964, 42 U.S.C.A. § 2000e *et seq.*, and the New Jersey Law Against Discrimination, N.J.S.A. 10:5-1 *et seq.*
51. *See* p. 46 of this article referring to the SDN list.
52. 15 U.S.C.A. § 1681 *et seq.*
53. C. App. A:9-79 *et seq.* Available at www.njleg.state.nj.us/2006/Bills/PL06/101_.PDF.
54. Senate Law and Public Safety and Veterans' Affairs Committee Statement to Senate Committee Substitute for Senate, Nos. 462 and 1289 (March 2, 2006), available at www.njleg.state.nj.us/2006/Bills/S0500/462_S1.HTM.
55. N.J.S.A. 13:1K-19 *et seq.*
56. *See* P.L.2001, c.246 (C.App.A:9-82), *supra*, note (45).
57. *See* Patriot Act, §§ 202, 209, *supra*, note (6).
58. *See* Patriot Act, § 215, *supra*, note (6).

*investigations, commercial disputes, and hospital and medical staff governance. She is a former New Jersey public advocate, public defender, and attorney general. **Khizar A. Sheikh** is an associate of Lowenstein Sandler PC, and concentrates his practice in state and federal civil and criminal matters, including general litigation, securities litigation, white-collar criminal defense, and internal investigations.*

Zulima V. Farber is a member of Lowenstein Sandler PC, and concentrates her practice in a wide variety of state and federal civil and criminal matters, including employment law matters, internal