

# **K&L** Alert

## EMPLOYMENT LAW

OCTOBER 2001

### Employer Security Checks on Employees: Permissible and Impermissible Use of Immigrant Status and National Origin

#### INTRODUCTION

The unthinkable events of September 11, 2001 have left an indelible mark on this country as on the entire world. As we now know, terrorists can live and work in this country for a number of years without detection, sometimes using falsified identity papers to enter and move about this nation, as well as to obtain employment. That fact, in and of itself, has placed Employers in a new and rather precarious position. To protect the security of their employees and businesses, Employers now are under ever-increasing public and political pressure to engage in heightened security checks of their employees and to implement other safety-related measures.

Determining the proper and legal way to do so, however, can be a difficult matter. Employers who single out employees because of their immigrant status, their national origin, or their religion risk violating various federal and state anti-discrimination laws, including the Immigration Reform and Control Act of 1986 ("IRCA") and Title VII of the Civil Rights Act of 1964 ("Title VII"). Indeed, the Equal Employment Opportunity Commission ("EEOC") recently issued a number of advisements to Employers, urging them to promote tolerance in the workplace in the wake of the terrorist attacks. So that Employers may be better prepared to recognize and address these difficult issues in the coming days, we have set forth below some guidelines for navigating the applicable statutory provisions in this complex and sensitive area, as well as some practical measures that can be implemented to bring about a safer, more secure workplace.

#### IRCA: EMPLOYMENT VERIFICATION AND ANTI-DISCRIMINATION

IRCA requires Employers to attest, under penalty of perjury, that they have examined their employees' documentation and have verified each employee's identity and eligibility to work in the United States. IRCA and its regulations provide three lists of documents that may be used to that end: (i) List A, documents that establish both identity and employment eligibility (such as a United States passport, a foreign

passport with a temporary I-551 stamp, or permanent resident card); (ii) List B, documents that establish identity only (such as a driver's license or an identification card issued by a federal, state, or local government agency); and (iii) List C, documents that establish employment eligibility only (such as a Social Security card, a United States birth certificate, or an unexpired employment authorization document issued by the Immigration and Naturalization Service ("INS")). Employers must verify that each employee has produced either (a) one valid document from List A, or (b) one valid document, each, from List B and List C.

IRCA prohibits discrimination on the basis of citizenship status and national origin. Although IRCA permits an Employer to give preference to a United States citizen over an equally qualified non-citizen, such preferences might violate Title VII.

#### SCOPE AND COVERAGE OF TITLE VII

Title VII prohibits adverse employment actions taken on the basis of an individual's race, color, religion, sex, or national origin. The EEOC and most circuit courts that have addressed the issue consider even undocumented, unauthorized workers to be protected by the provisions of Title VII. Employers, of course, also must be cognizant of the state anti-discrimination laws in effect in the various states in which they operate, the scope and coverage of which may differ in important ways from those of Title VII.

#### SPECIFIC EXCLUSIONS FROM "UNLAWFUL EMPLOYMENT PRACTICES"

Sadly, the events of September 11 were not the first or only national emergency that this nation has encountered. Embedded in Title VII are congressional responses to historical crises. For example, Title VII provides that it is not an unlawful employment practice to take adverse employment actions against members of the Communist Party of the United States or of any other pro-communist organization. Title VII also excludes from the definition of

“unlawful employment practice” any action taken against an employee if that employee’s position or duties are subject to any requirement imposed in the interest of national security under any statutory or Presidential national security program.

To date, however, no such national security program has been implemented addressing international terrorism, nor has Title VII been amended to exclude from the definition of “unlawful employment practice” employment actions against certain groups allegedly associated with terrorism. The law may be moving in that direction, however. On September 24, 2001, for example, Attorney General Ashcroft presented to Congress his outline of a proposed Mobilization Against Terrorism Act, which, in its final form, may impact the employment laws as noted above. Until that Act or others like it are implemented, however, Employers still must operate within the confines of Title VII as it currently exists.

#### **SECURITY MEASURES: PRACTICAL STEPS**

Employers, with the guidance of their employment counsel, should design and implement their workplace security programs against the backdrop of this statutory framework. So, too, should they be aware of myriad other laws that may be implicated by such programs. To aid in such efforts, we offer the following suggestions for certain practical steps that can be implemented — and certain pitfalls that must be avoided — to create a safer and more secure workplace.

*Identify your particular security needs and concerns.* No two Employers will have the same security needs. The new face of terrorism thrives on secrecy, anonymity, and the ability to infiltrate ordinary but vulnerable walks of American life. The first and most critical step for every Employer to take is to identify its own particular security needs and concerns, for its business in general and, indeed, for each location at which it operates. In designing a security program, Employers should keep in mind such factors as the following: (i) the nature of their business, including whether it involves or interacts with the defense industry, the chemical industry, the travel business, communications, intelligence, or other potential “targets” of international terrorism; (ii) the nature of the products that are handled in day-to-day operations, including whether any products can be used for destructive purposes; (iii) the size of the workforce at each location, including whether all employees are easily recognizable without identification; (iv) the number of employees who come in contact with potentially hazardous or dangerous materials; (v) the degree to which employees interact with the public and the ability of members of the public to enter the workplace unnoticed; (vi) the turnover rate of employees; (vii) any known “soft spots” or particular concerns with respect to security; and (viii) whether there have been any “close calls” in which disasters, intentional or accidental, were narrowly avoided. The list goes on and on. No one knows better than Employers how to isolate and address the security needs of each workplace location.

*Review and update your background and security checks of new hires.* The most effective way for Employers to keep security threats from their workforce is not to hire persons who are legitimate security threats as employees in the first place. A thorough review and update of your background and security check policies, therefore, is extremely important. The following issues, however, must be considered.

- *IRCA Issues.* Although Employers have an obligation not to hire persons who present falsified employment documentation, as long as the documents presented are prescribed by IRCA and appear to be facially genuine, Employers must accept them and may not lawfully require the employee to produce any documents or information in addition to them. Further, the mere fact that an employee is of a particular national origin or practices a particular regional religion most likely will be an insufficient basis for an Employer to expose that employee’s documentation to heightened scrutiny. Employers, however, may use a third-party specialist to review employment documentation to ensure more effectively the authenticity of that documentation, but they must take care not to do so on a discriminatory basis (e.g., only doing so for applicants of Arab descent).
- *Title VII Issues.* It goes without saying that Employers may not refuse to hire persons because of their race, religion, or national origin. It also most likely would be a violation of Title VII for an Employer to subject applicants to heightened background and security checks on the basis of a protected trait. We encourage Employers to implement more thorough background and security checks, but, absent a legitimate and identifiable security concern, such checks must be performed on a non-discriminatory basis. Employers who are government contractors also should keep in mind whether they have complied with any affirmative action plan that is in place.
- *FCRA Issues.* Employers may desire to retain third-party private investigators to perform background and security checks of their applicants for employment. Although that practice, in and of itself, does not violate IRCA or Title VII, it nevertheless may implicate the notice and disclosure requirements of the Fair Credit Reporting Act (“FCRA”) and similar state laws. Those requirements will be triggered if the Employer makes employment decisions based upon information gathered bearing not only on credit worthiness, but also on character, general reputation, and personal characteristics. We suggest that, if such a practice is undertaken, Employers should obtain signed releases at the time of hiring that cover future “consumer reports,” as well, which may obviate the need to notify employees of such reports during later stages of the employment relationship. If the Employer intends to initiate a more intrusive “investigative consumer report,” however, which includes personal interviews with the applicant’s neighbors, friends,

and associates, then the Employer must mail written notice to the applicant within three days of requesting the investigation and inform the subject of his or her right to know the nature and scope of the investigation.

*Design and implement a review of your current employees' employment records.* Another important security measure for Employers is to ensure that their existing workforce is free from legitimate security threats. Again, various anti-discrimination issues arise.

- **IRCA Issues.** The INS and the Department of Labor are authorized, on their own initiative, to conduct investigations of Employers' employment verification practices and procedures to ensure compliance with IRCA. Employers, too, are under an ongoing obligation to ensure that they are compliant with IRCA. Yet, the issue becomes more complicated when choices need to be made as to which employees' records to review to confirm such compliance. As with applicants and new hires, national origin most likely will be an insufficient basis for an Employer to take a "second look" at an employee's employment documentation. It appears that Employers, though, would be entitled to perform any number of non-discriminatory audits of their employees' work authorization papers without violating the provisions of IRCA, such as universal audits of the work authorization papers of all employees or periodic random audits of work authorization papers. Of course, the permissibility of such reviews would have to be analyzed in the context of the facts of any given situation.
- **Title VII Issues.** If an Employer is only reviewing its employees' employment records and no further action is taken, that action most likely would not rise to the level of an adverse employment action. If any action is taken against an employee based upon that review, however, then the process by which employees are selected to have their records reviewed becomes critical. Subject to the caveat below, non-discriminatory, facially neutral reviews most likely would not violate Title VII, such as universal reviews of all employees' records or periodic random reviews of records. By contrast, reviews performed on the basis of national origin (for example, if an Employer reviews only the employment records of its employees of Middle Eastern background) or, indeed, upon anything less than a true, palpable security concern, pose a serious risk of violating the law if they result in an adverse employment action. After the Iranian hostage situation in the late 1970s, for example, some Employers defended actions taken against employees and applicants of Iranian background on the basis of that crisis. That defense, however, was rejected by federal courts. Such cases confirm that, under Title VII, adverse employment actions may not be taken on the basis of national origin alone as a "proxy" for a purported national security concern.

One caveat that Employers should keep in mind when designing and implementing a security review is that, even if such a review is facially neutral, Employers still may face liability for disparate impact discrimination if that review results in a disproportionate negative effect on a protected group and cannot be justified by a business necessity. Employers will have to defend such claims by proving that their security review practices are job-related and consistent with a business necessity. We recommend a prompt review of all security-related policies and practices to ensure that they are narrowly tailored to an articulated business necessity.

The issues surrounding the conduct of security checks by private Employers do not directly implicate issues of "racial profiling," which most typically arise in the area of Fourth Amendment search and seizure law and, thus, are not applicable to private sector Employers. Yet, the similarities are undeniable, and the leeway recently given to police authorities in identifying persons suspected of criminal activity on the basis of a racial or other "profile" may be instructive as to how the INS and the EEOC may deal with similar issues in the workplace.

- **FCRA Issues.** Undertaking reviews of documentation by a third-party investigator, again, most likely will trigger the notice and disclosure requirements of the FCRA and similar state laws. If a valid waiver and release concerning "consumer reports" was obtaining at the commencement of employment, additional notice most likely will not be required. Notice and disclosure will be required for any "investigative consumer reports."

*Determine the security risks of your business on a position-by-position basis.* Some positions present more of a security risk than others. By identifying now the positions that pose the most serious threats and designing a security program accordingly, Employers can reap certain important and ongoing benefits. Specifically, identifying positions as highly sensitive to security may, to a considerable extent, essentially define certain security measures into the job descriptions for those positions and will help Employers articulate a legitimate, non-discriminatory reason for undertaking heightened security measures for particular positions. Additionally, to the extent that Employers are able to describe a legitimate business necessity with respect to security measures for certain positions, it will aid in designing a security program that will have a greater chance of defeating any disparate impact challenge. A focused security program also will help Employers economize on resources in implementing their programs.

*Review and update your anti-discrimination and anti-harassment policies.* At present, when charges of discrimination and harassment are likely to be on the rise, it is critical for Employers to have current and updated anti-discrimination and anti-harassment policies and

procedures. Employers should review those policies and procedures with their employment counsel to ensure that they specifically address not only race, sex, and age discrimination, but also discrimination on the basis of national origin, religion, and ethnicity. Employers should remind their workforce, whether through meetings, memoranda, or other effective communications, that all types of discrimination are prohibited. Complaint procedures also should be reviewed and updated to ensure that they provide a clear, effective, and well-advertised means for reporting allegations of unlawful discrimination.

*Establish lines of communication with the authorities.* If an Employer takes information gathered through background checks and, rather than taking action on its own, simply reports that information to the proper authorities to allow them to take official action if the authorities determine that such action is necessary, such conduct by the Employer may not constitute an adverse employment action. Although that may allow the Employer to avoid liability under Title VII and IRCA, however, it raises still further issues regarding the employees' privacy interests, which also must be protected. Ultimately, a balancing of those privacy interests with the legitimate security interests of the Employer and the authorities will need to be performed in each situation. In any event, simply making contact with authorities prior to a security situation developing to open the lines of communication and to establish and confirm emergency procedures will help to minimize response time if such an unfortunate incident ever arises.

*Review and update your disaster recovery plan.* The magnitude of the impact of the events of September 11 on businesses is difficult to comprehend and may not be fully understood for years. The loss of paper and information in the tragedy cannot be compared to the loss of life. Yet, in our attempt to carry on with business, now more than ever we know that having a disaster recovery plan is extremely important. A full review and updating of such plans is warranted.

*Implement other security measures tailored to your business.* Employers have at their disposal still other security measures, as well, the effectiveness of which will depend upon the particular situation at each workplace. For example, such measures might include: (i) implementing more stringent policies against the carrying of weapons on company property, including pocket-knives and other

“concealed” weapons; (ii) limiting and monitoring non-business use of computers, electronic mail, and the internet; (iii) reviewing and improving the security of hazardous materials in the workplace; (iv) requiring employees to wear ID badges (Employers should take care what information to include on such badges); (v) restricting employee and visitor parking to areas further away from company buildings; (vi) restricting access to security-sensitive locations to specifically authorized employees; (vii) installing metal detectors at employee entry points; (viii) implementing more stringent policies against the carrying of boxes, large bags, or other carrying cases; and (ix) retaining third-party security personnel where appropriate, or reviewing the capabilities and effectiveness of any existing security personnel. We suggest reviewing or designing a complete security program in a manner that ensures effectiveness and compliance with applicable law.

## CONCLUSION

For now, Employers must deal with a changed world under the governance of employment laws which have not yet caught up with today's circumstances, but which will surely do so before long. As set forth above, although Employers must take care not to engage in shortsighted reactionary measures, there are particular, identifiable steps that Employers may take to preserve their own security while still not violating the employment laws as they currently exist.

---

### STEPHEN M. OLSON

412.355.6496  
solson@kl.com

### DAVID J. KOLESAR

412.355.6252  
dkolesar@kl.com

If you would like to discuss any of these issues, please contact the authors or any of the following K&L employment lawyers:

Boston	Henry Goldman	617.261.9156	hgoldman@kl.com
Dallas	Amy Bourret	214.939.4951	abourret@kl.com
Harrisburg	Carleton Strouss	717.231.4503	cstrouss@kl.com
Los Angeles	Thomas Petrides	310.552.5077	tpetrides@kl.com
	Paul Sweeney	310.552.5055	psweeney@kl.com
Miami	Daniel Casey	305.539.3324	dcasey@kl.com
Newark	Anthony La Rocco	973.848.4014	alarocco@kl.com
New York	Loren Schechter	212.536.4008	lschechter@kl.com
Pittsburgh	Stephen Olson	412.355.6496	solson@kl.com
	Michael Pavlick	412.355.6275	mpavlick@kl.com
	Hayes Stover	412.355.6476	hstover@kl.com
San Francisco	Charles Thompson	415.249.1017	cthompson@kl.com
Washington	Lawrence Lanpher	202.778.9011	llanpher@kl.com



**Kirkpatrick & Lockhart LLP**

*Challenge us.*

BOSTON ■ DALLAS ■ HARRISBURG ■ LOS ANGELES ■ MIAMI ■ NEWARK ■ NEW YORK ■ PITTSBURGH ■ SAN FRANCISCO ■ WASHINGTON

This publication/newsletter is for informational purposes and does not contain or convey legal advice. The information herein should not be used or relied upon in regard to any particular facts or circumstances without first consulting with a lawyer.

© 2001 KIRKPATRICK & LOCKHART LLP. ALL RIGHTS RESERVED.