

INTERNATIONAL

April 2019

EXPECT FOCUS[®]

LEGAL ISSUES AND DEVELOPMENTS FROM CARLTON FIELDS

WHAT LIES
AHEAD

NAVIGATING
IN AN
UNCERTAIN
FUTURE



**CARLTON
FIELDS**

EXPECTFOCUS® International is a review of legal issues and developments related to international business, provided on a complimentary basis to clients and friends of Carlton Fields.

The content of EXPECTFOCUS® is for informational purposes only and is not legal advice or opinion. EXPECTFOCUS® does not create an attorney-client relationship with Carlton Fields or any of its lawyers.

EXECUTIVE EDITOR

Andrew J. (Josh) Markus

EDITOR

Barry Leigh Weissman

PRODUCTION MANAGER

Jessica Bennett

ART DIRECTOR & DESIGNER

Frances Liebold

CONTRIBUTORS

Steven Blickensderfer
Florence Druguet
Maria Mejia-Opaciuch
Arnaldo Rego
Joseph Swanson

Table of Contents

- 3 Foreign Investment Review Becomes Communitywide
- 4 Brazil's New Data Protection Law: An Overview and Four Key Takeaways for U.S. Companies
- 7 Brexit This Way
- 8 Cross Your T's and Dot Your I-9s During an M&A Transaction
- 10 Mergers and Acquisitions: Seal of Approval on Work Visas

SUBSCRIPTIONS

Changes in address or requests for subscription information should be submitted to:

Peggy Bourque, pbourque@carltonfields.com.

Copyright © 2019 Carlton Fields. All rights reserved. No part of this publication may be reproduced by any means, electronic or mechanical, including photocopying, imaging, facsimile transmission, recording, or through any information storage and retrieval system, without permission in writing from Carlton Fields. EXPECTFOCUS® is a registered trademark of Carlton Fields, P.A.



EXPECTFOCUS.COM

Foreign Investment Review Becomes Communitywide

BY ANDREW J. (JOSH) MARKUS

Following up on the Foreign Investment Risk Review Modernization Act (FIRRMA), the United States' amendment to the Committee on Foreign Investment in the United States (CFIUS), the European Union (EU) has now enacted a new framework for screening foreign direct investment into EU states. The authority to screen foreign direct investment in the EU lies with each nation state. But in the spirit of formalizing a harmonized approach to screening, the EU has enacted the Regulation on Foreign Direct Investment Screening (FDI Regulation). The European Parliament approved this measure, and it will become effective on October 11, 2020.

Foreign direct investment review legislation is currently in place in 12 of the 27 members of the EU. The FDI Regulation is aimed at investments that are made directly by non-EU persons or entities into EU businesses. It is not intended to include portfolio investments.

The FDI Regulation sets out a list of factors to be considered in foreign investment reviews. As with many regulations, the FDI Regulation is intended to encourage uniformity in investment review. Among other things to be considered by governments, critical infrastructure and technology as well as sensitive information will be considered in investment reviews.

The intent of the FDI Regulation is to require EU state governments to report on their reviews of foreign direct investment transactions. The FDI Regulation requires a government to inform the EU and the member states of any investment that is undergoing screening. If at least one-third of member states consider the investment to be likely to affect security or public order, the European Commission may issue a non-binding official opinion regarding whether the investment is likely to affect EU nations' security or public order. While the opinion is not binding, it is an official pronouncement of the Commission. And if a government decides not to follow the opinion, the FDI Regulation requires it to provide an explanation of why it did not follow the opinion.

The effect of the FDI Regulation inside the community is to: (1) promote cooperation among EU nations; (2) allow member states to possibly influence the direction of foreign direct investment into the EU; (3) potentially harmonize investment review legislation in member states; and (4) establish an oversight mechanism that will attempt to promote security and avoid investment that will contravene established norms (ordre publique). Will this become, as some people view the GDPR, an anti-competitive obstacle to foreign investment in EU businesses?

What it definitively means for investors is unknown. But our guess would be that it means a number of things for investors, none of them extremely good. First, as in the United States under FIRRMA, more investments will come under scrutiny. Second, more information will be sought by government review bodies, causing expense, delay, and possible confidentiality issues. Third, potentially sensitive investments will need to consider an extended review timetable and, possibly, interference by national review bodies as well as EU member states. Finally, if there is a possibility of intervention by one-third of the member states and a non-binding opinion by the European Commission, will investors shy away from making an investment in the first place or will the absence of such intervention become a standard condition to the closing of non-EU investments into the EU.

Apparently, as the United States goes, so goes the world. This new FDI Regulation seems to underlie a movement toward sovereignty in all aspects of the regulation of investment. It is also a recognition of the changing environment in which we live and another step toward what Jean Monnet and Robert Schuman envisioned as the ultimate goal of the European integration movement — political as well as economic integration.



Brazil's New Data Protection Law: An Overview and Four Key Takeaways for U.S. Companies

BY STEVEN BLICKENSDECKER, JOE SWANSON AND ARNALDO REGO

2018 was a watershed year for data privacy regulation. While Europe's General Data Protection Regulation (GDPR) and California's Consumer Privacy Act (CCPA) garnered the most attention from the public and businesses worldwide, Brazil also passed a new privacy law that makes sweeping changes to its existing data protection regime and promises to impact many businesses operating there, even those without a physical presence in Brazil.

In August 2018, Brazil passed its first comprehensive data protection regulation, the Lei Geral de Proteção de Dados (General Data Protection Law, or LGPD). Like the GDPR, the LGPD imposes new rules regarding the collection, use, processing, and storage of personal data in electronic and physical

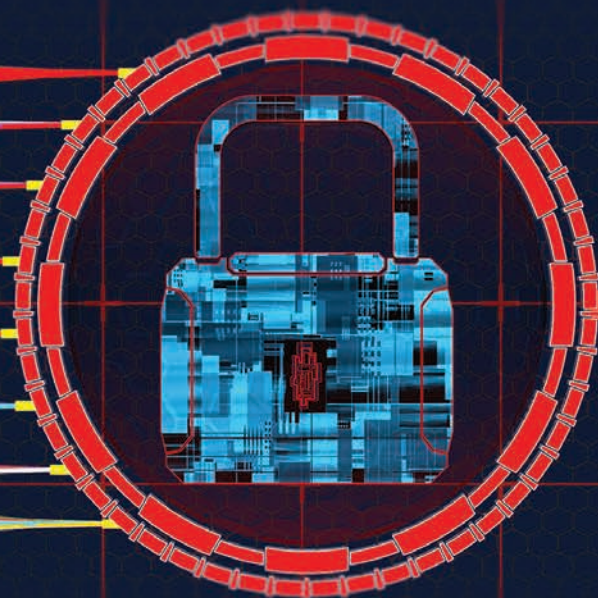
This article is intended to help businesses understand the LGPD and its effects by: (1) providing a general overview of the rights and obligations the LGPD creates and the scope of its application and extraterritoriality; (2) highlighting notable differences from the GDPR; and (3) presenting key takeaways for businesses in the United States that may be affected by this new regulation.

What Does the LGPD Regulate?

The LGPD regulates the collection and use of "personal data," defined

form and will affect all industries and sectors of the Brazilian economy. Before the LGPD, the data protection regulatory framework in Brazil was sector-based and primarily regulated by the country's Civil Rights Framework for the Internet (Internet Act) and Consumer Protection Code, among others. Shortly after passing the LGPD, Brazil provisionally created the Brazilian National Data Protection Authority to enforce the LGPD, and extended the compliance period to August 2020.

broadly as information relating to an identified or identifiable natural person, in both digital and non-digital form. Unlike many other privacy laws, this definition does not include examples of "personal data." The LGPD further regulates "sensitive personal data," which is defined as data relating to racial or ethnic origin, religious belief, political opinion,



union membership, philosophical or political organization, health, sexual orientation, and genetic or biometric data.

There are notable exceptions to the law's application to personal data, much like the GDPR. The LGPD generally does not apply to processing of anonymous data or personal data used for household, artistic, journalistic, academic, or national security purposes. The law also does not regulate business-to-business (B2B) information.

Whom Does the LGPD Affect?

Like the GDPR, the LGPD regulates controllers and processors of personal data. Controllers are the natural or legal entities who decide how and why to collect and process personal data. Processors are the entities who process the data according to the controller's instructions.

Much like the GDPR and the CCPA, the LGPD applies across industry sectors and has extraterritorial application. There are two main aspects to its application. The LGPD applies to any individual or organization, private or public, regardless of residency:

1. collecting or processing personal data in Brazil; or
2. intending to offer or provide goods or services to individuals in Brazil.

fundamental rights and freedoms of the data subject. These differences arguably make the LGPD more flexible in terms of justifying the processing of personal data when compared to the GDPR.

All organizations governed by the LGPD as controllers will also need to appoint a data protection officer, absent future clarifications from the Brazilian National Data Protection Authority. This differs from the GDPR, which only requires a data protection officer in certain circumstances. Data protection officers do not need to be natural persons, meaning companies can serve in that capacity, and it is unclear whether they need to reside in Brazil. The appointment of a data protection officer may be a new and unexpected expense for some companies, particularly those in the

Thus, a business collecting or processing personal data need not be headquartered, or even have a physical presence, in Brazil for the LGPD to apply. The consequences of non-compliance with the LGPD can be just as severe as non-compliance with the GDPR. Violations of the LGPD can result in fines of up to 2 percent of the company's gross revenues derived from Brazil, or 50 million reais (approximately \$13 million), per infraction.

United States without a presence in Brazil or the EU. The LGPD, however, does not require the designation of a representative in Brazil in the same way the GDPR requires one for United States businesses offering goods and services in the EU.

How Does the LGPD Differ From the GDPR?

Although inspired by the GDPR, the LGPD and the GDPR differ in several notable ways. First, the LGPD includes additional legal bases for processing personal data than the GDPR, such as an additional basis related to the protection of credit. Second, with respect to the "legitimate interest" legal basis for processing, which is provided in both laws, the LGPD's standard is satisfied where the processing of personal data can be shown to support and promote the controller's activities after balancing the data subject's privacy rights. Under the GDPR, the legitimate interests of the controller cannot override the

It is also uncertain whether the LGPD will require data processing agreements between the collectors and processors, as is required by GDPR Article 28. There is no functional equivalent of GDPR Article 28 in Brazil's new law. Nevertheless, it is recommended to implement a data processing agreement so that

the parties fully understand their respective responsibilities with respect to the collection, use, and protection of personal data, and if there is ever an incident involving personal data. This is particularly true under the LGPD, where liability is joint and several absent an agreement limiting a processor's liability.

Additionally, when it comes to reporting data breaches to the data protection authority, the LGPD requires reporting within a "reasonable time." This is considered less rigid than the GDPR's 72-hour deadline.

Key Takeaways

There are four key takeaways for U.S.-based businesses evaluating whether, and to what extent, the LGPD affects their business.

2. The LGPD, again like the GDPR and the CCPA, does not apply to non-personal data, such as B2B data. A good first step for any business asking whether these data protection laws apply is to conduct a data-mapping analysis to understand the different types of data flowing into the business from inception through the end of the data's life cycle. A proper data map requires input from the business's data-driven departments, such as marketing and human resources.
3. It is important to remember that the LGPD, like the GDPR and the CCPA, is technology-blind and does not hinge on whether personal data is in hard copy or digital form. These statutes are intended to apply for years to come, regardless of the
4. A business that has implemented measures to comply with the GDPR and the CCPA can use many of the same measures to comply with the LGPD. For example, the mechanisms through which a business responds to subject access requests (SARs) are largely the same. Moreover, while the LGPD does not specify that data processing agreements are required, entering into such agreements will aid in demonstrating compliance and protecting your business's interests.

Questions?

Businesses have until August 2020 (in the event the provisional measure is ratified) to come into compliance with the LGPD. And many of the

1. The LGPD, like the GDPR and the CCPA, applies extraterritorially, meaning it impacts businesses that do not necessarily have a physical presence in Brazil. The key questions in determining whether the LGPD applies to a U.S.-based business are: (1) whether any data collection or processing activities occur in Brazil; and (2) whether the business intends to offer or provide goods or services to individuals in Brazil. If a business satisfies either factor, then all of the LGPD's provisions apply.

changes in technology. This is already proving to be a challenge for industry-altering forms of technology, such as artificial intelligence and blockchain technologies. Businesses should keep this in mind when determining whether and to what extent these laws apply to their data collection and processing activities, and when determining whether to engage in new products and services.

actions companies are taking to demonstrate compliance with the GDPR can be used to demonstrate compliance with the LGPD. If you have questions about the LGPD and whether it applies to your business or compliance, please contact the authors of this article.



Brexit This Way

BY BARRY WEISSMAN AND FLORENCE DRUGUET

If Brexit happens, it will impact the entire European Union (EU) in various ways, and not just economically. For instance, what about the expatriates from an EU country residing in the U.K. pursuant to the current EU immigration rules or the 1.4 to 1.8 million U.K. nationals living in an EU country, like France, pursuant to the same EU immigration rules? Depending on whether a Brexit with an agreement (“Soft Brexit”) or without one (“Hard Brexit”) occurs, a lot of retirees could be forced to move back to the U.K., which would likely result in overburdening the U.K.’s health and retirement systems.

Under a Hard Brexit, the U.K. will no longer be required to abide by the same laws and courts as EU members. Businesses will no longer be able to move freely between the EU and the U.K. Indeed, since U.K. businesses will most likely lose full access to the EU single market (whether it is a Hard or Soft Brexit), companies are already hesitating to use the U.K. as a base for their investment in the EU market, resulting in an exodus of EU residents and businesses from the U.K. and potentially a real estate collapse.

Unfortunately, what a Brexit really means is completely unknown. What is certain is that a Hard Brexit would leave the U.K. and the EU without any trade agreements, forcing them to default to the World Trade Organization. Hence the urgency for U.K. officials to negotiate a trade deal with the EU. For the U.K. to leave the EU, it had to invoke Article 50 of the Lisbon Treaty, which gave the U.K. and the EU two years to agree on the terms of an exit plan. Prime Minister Theresa May triggered this process on March 29, 2017. The result of the trigger is that the U.K. was originally scheduled to leave at 11 p.m. U.K. time on March 29, 2019. However, because the parties could not come to an agreement by March 29, Prime Minister May and EU leaders negotiated a two-week delay, moving the deadline to April 12. Even this is uncertain given recent elections in Parliament and the growing movement to have another referendum on whether there should even be a Brexit.

This time of uncertainty has a great impact on businesses looking to open, acquire, merge, or invest in EU or U.K. entities. No one really knows what is actually going to happen. The 21-month transition plan negotiated by Prime Minister May and the EU in March 2018 was defeated by the British Parliament in January, February, and March 2019. Since the defeat, Prime Minister May has not been able to come to an agreement with the divided British Parliament. Out of fear, and in an attempt to minimize the impact in case of a Hard Brexit, the U.K. signed a bilateral trade agreement with Switzerland to lift tariffs in the event of a Hard Brexit.

One of the important terms for a Soft Brexit is the amount of money the U.K. would be required to pay to the EU for the right to leave. Prime Minister May had earlier agreed to pay approximately \$50.7 billion for an organized Brexit. However, given the present political climate, one cannot predict whether there will be a Brexit, or what type it will be if it does occur, and whether Parliament will foot the \$50.7 billion bill.

If there is no Brexit, the U.K. will continue to pay approximately \$206 million a week, or \$10.2 billion a year. Clearly, these numbers indicate the tremendous impact of an exit for both the U.K. and the EU. It also indicates one of the justifications for the EU’s hard stance during those

negotiations. The U.K. contributes 13 percent of the entire EU budget, and it is unknown how or where the EU will find another source for these moneys if the U.K. leaves. If the U.K. does leave the EU, the EU has prepared a “no-deal” Contingency Action Plan that will be implemented on the day the U.K. leaves the EU. The British and Irish governments have also prepared plans.

Another uncertainty in a Hard Brexit is whether U.K. businesses and the British government will be able to conduct investigations and prosecutions outside of the U.K., and for the EU to conduct them in the U.K. This means there is both a political fear and business concern about an increase in fraud and the inability to prosecute it, either civilly or criminally.

Today the British political branch is in turmoil. Petition for a second referendum is getting even more support, and a second public vote would need Parliament’s approval. Even so, as of today, it is unclear whether there would be enough time or support for it.

Assuming there will be a Brexit, regardless of whether it is Hard or Soft, doing business in the present U.K. and EU is going to be somewhat perilous and clearly more expensive and risky than in the past.

Cross Your T's and Dot Your I-9s During an M&A Transaction

BY MARIA MEJIA-OPACIUCH

In a merger, acquisition, or reorganization of any business, transactional lawyers have an obligation to review a critical area to avoid serious consequences to the acquiring company: immigration issues and, specifically, Form I-9s.

Federal law requires that employers verify the employment authorization of all employees, citizens and noncitizens alike, by completing U.S. Citizenship and Immigration Services (USCIS) Form I-9 ("Employment Eligibility Verification," revised July 17, 2017) for each employee at the time of hire. The form is used to verify an employee's identity and work authorization.

Examining I-9s of the acquired company is important for a variety of reasons, namely: (1) the information on the I-9 provides an overview of the acquired company's workforce; and (2) a review of the I-9 will reveal the acquired company's compliance with federal law and the company's internal I-9 policy and program, if any. This review will enable the acquiring company to determine if it is assuming potential liabilities for noncompliance resulting in severe monetary fines, and possibly criminal penalties.

The USCIS permits employers who have acquired another company or who have merged with another company to treat employees who are continuing their employment with the related, successor, or regionalized employer as:

- New hires, and thus the acquiring employer must complete a new I-9; or
- Continuing in employment, and thus the acquiring company must obtain and maintain the previously completed I-9.

Employers choosing to complete a new form may do so before the merger or acquisition takes place as long as the acquiring employer has offered the acquired employee a job and the employee has accepted the offer. The employee must complete Section 1 of the form no later than the first day of employment, and the employer or the authorized representative must complete Section 2 of the form within three business days thereafter. Employers should enter the effective date of the acquisition or the merger as the date the employee began employment in Section 2 of the new I-9.



Employers choosing to keep the previously completed I-9 accept responsibility for any errors or omissions on those forms. Employers should therefore review each I-9 with the employee and update or reverify the employee's information as necessary and legally required. Typically, 50 to 70 percent of a company's paper I-9s have some kind of error. Common errors are either paperwork errors (e.g., no dates, no signatures, or incomplete forms) or technical violations such as using the wrong version of the form or failing to complete a form for a current employee.

On February 3, 2017, civil penalties increased for any violations, paper or technical, occurring after November 3, 2015. The civil fines can add up quickly now that the potential liability for paperwork violations can come with a price tag ranging from \$224 up to \$2,236 per violation where there is a pattern of such violations. In a workforce of 2,000 employees, where 50 percent of the I-9s have such violations, the fines could be well over \$2 million.

Due to these hefty fines, possible criminal penalties where there is intent to hire and employ workers without authorization, bad press, and a decrease in the value of the acquisition, the acquiring company should ask the following questions before the deal closure when reviewing the acquired company's I-9s:

1. Does an I-9 exist for every employee of the company? Check payroll records against the I-9s.
2. Have the I-9s been fully and correctly completed?
3. Does the acquired company have a written I-9 policy? Is there one that can be incorporated into the buyer's policy and applied uniformly across the new company?

4. If the I-9s contain errors, are they technical or substantive errors?
5. What are the potential civil fines or criminal penalties?
6. Should the acquiring company complete new I-9s or retain the old ones and assume liability?

Answers to all of these questions will help develop a plan to move forward and avoid severe liability. And depending on the results of the I-9 review, an internal audit of the I-9s may need to be conducted to correct error-ridden I-9s while the workforce is still accessible. Correcting I-9s while an employee is available is the soundest way to proceed. With the increase in both I-9 enforcement and the pace of corporate mergers and acquisitions, buyers should beware of potential I-9 liabilities before closing a deal.



Mergers and Acquisitions: Seal of Approval on Work Visas

BY MARIA MEJIA-OPACIUCH


2019 is showing to be a strong year for continued activity in the mergers and acquisitions arena. There is an uptick from a year ago this time, and surveys on the corporate side and on the private equity side continue to be optimistic for more deal flows in 2019. Such corporate restructurings raise legal issues in the employment sector. Buyers in these transactions may fail to consider the immigration issues that arise as a result of a merger, an acquisition, or even a restructuring. The Form I-9 compliance is a key concern, as is the use of E-Verify.

Furthermore, it is important to note that the sale of a company may result in any of that company's foreign national employees on temporary work visas — specific to their employer, the location, or the particular position — to lose the ability to continue to work in the United States legally. Such a sale would lead to a loss of employment authorization and leave the employees in the United States in violation of their work visa status. Additionally, the new employer cannot legally have these foreign national employees on its payroll, as doing so would violate immigration laws. The new employer would have foreign national employees working in the United States without authorization and, thus, not in compliance with U.S. immigration laws. It is important to review the transaction to determine if it is a stock purchase or an asset purchase. A stock purchase is less likely to trigger a foreign national employee's loss of employment authorization versus an asset purchase, which is more likely to prompt a loss of employment authorization among foreign nationals following any type of corporate restructuring.

To avoid an illegal employment situation and a possible decrease in the value of the corporate transaction — both of which result in a bad outcome for the buyer — it is essential to conduct due diligence of all employment authorization issues before closing a deal.

Buyers should gather information and documentation, as listed below, before the closing of the transaction and consult experienced business immigration and employment counsel to review and develop a plan to maintain work authorization through the sale of the company:

1. A list of employer-sponsored employees, those who are dependent on the seller for authorization to work and reside legally in the United States and who may lose that work authorization if no longer employed by the seller.
2. A list of immigration cases currently in process, whether on a temporary work visa or in the process of seeking permanent residence (indefinite employment) in the United States via the U.S. Department of Labor (DOL), the U.S. Citizenship and Immigration Services (USCIS), or the U.S. Department of State (DOS). The most likely work visas buyers would encounter are as follows:
 - a. E-1 and E-2 Treaty Trader and Treaty Investor Visas are premised on a treaty between the United States and the foreign national employee's home country. The U.S. company must be at least 50 percent owned by nationals of the foreign country, and thus a restructuring may render the E-1 or E-2 visa unavailable to the foreign national employee.
 - b. L-1 Intracompany Transferee Visa is based on a qualifying relationship between the U.S. company and the foreign company for which the foreign national employee worked for one full year before the employee's transfer to the United States. If the corporate restructuring does not include the foreign company, then the L-1 visa may be lost.
 - c. TN Professional Visa is premised on the North American Free Trade Agreement (NAFTA) provisions for temporary work visas for certain professionals to work in the United States for a specific employer, and thus any corporate restructuring would require a new TN application

- 
- d. H-1B Specialty Occupation Visa is widely used for professionals working in the United States for a specific employer. To keep the foreign national employee whole in corporate restructurings involving a stock or asset purchase or hybrid arrangement, the buyer may need to step into the shoes of the seller and provide a sworn statement to accept the immigration obligations and liabilities of the seller. Otherwise, it is recommended that the buyer process a new H-1B petition for the foreign national employee. This is especially recommended where the buyer may make material changes to the H-1B employee's work site or job duties.
 - 3. A listing of any foreign national employees working for the company under the H-1B visa and a copy of the corresponding Public Access File (PAF) for that H-1B employee.
 - 4. A sampling of I-9 files for each and every location of the seller's work site and the copies of the supporting documents, if it is the seller's I-9 practice to keep such copies.

Gathering and reviewing all of the above documents, and developing a plan of action to maintain immigration compliance before any final corporate restructuring, will enable the buyer to protect itself. Today's administration is focused on audits, investigations, and enforcement. And with the continued rise of mergers and acquisitions, caution in due diligence of immigration matters will benefit both the buyers and their acquired workforce.



CARLTON FIELDS serves business clients in key industries across the country and around the globe. Through our core practices, we help our clients grow their businesses and protect their vital interests. The firm serves clients in nine key industries:

Life, Annuity, and Retirement Solutions
Banking, Commercial, and Consumer Finance
Construction
Health Care

Property and Casualty Insurance
Real Estate
Securities & Investment Companies
Technology & Telecommunications

For more information, visit our website at www.carltonfields.com.

Atlanta

One Atlantic Center
1201 W. Peachtree Street | Suite 3000
Atlanta, Georgia 30309-3455
404.815.3400 | fax 404.815.3415

Miami

Miami Tower
100 S.E. Second Street | Suite 4200
Miami, Florida 33131-2113
305.530.0050 | fax 305.530.0055

Tallahassee

215 S. Monroe Street | Suite 500
Tallahassee, Florida 32301-1866
850.224.1585 | fax 850.222.0398

Hartford

One State Street | Suite 1800
Hartford, Connecticut 06103-3102
860.392.5000 | fax 860.392.5058

New Jersey

830 Morris Turnpike | 4th Floor
Short Hills, NJ 07078-2625
973.828.2600 | fax 973.828.2601

Tampa

Corporate Center Three
at International Plaza
4221 W. Boy Scout Boulevard | Suite 1000
Tampa, Florida 33607-5780
813.223.7000 | fax 813.229.4133

Los Angeles

2000 Avenue of the Stars
Suite 530, North Tower
Los Angeles, California 90067-4707
310.843.6300 | fax 310.843.6301

New York

Chrysler Building
405 Lexington Avenue | 36th Floor
New York, New York 10174-3699
212.785.2577 | fax 212.785.5203

Washington, DC

1025 Thomas Jefferson Street, NW
Suite 400 West
Washington, DC 20007-5208
202.965.8100 | fax 202.965.8104

Orlando

SunTrust Center – Main Tower
200 S. Orange Avenue | Suite 1000
Orlando, Florida 32801-3400
407.849.0300 | fax 407.648.9099

West Palm Beach

CityPlace Tower
525 Okeechobee Boulevard | Suite 1200
West Palm Beach, Florida 33401-6350
561.659.7070 | fax 561.659.7368