TH QUARTER 2010, VOLUME 20, NUMBER 4

BANK DIRECTOR

CHARTING A COURSE FOR AMERICA'S BANKING LEADERS

WELCOME TO THE GREAT UNKNOWN

Dodd-Frank is raising more questions than answers among banks and their boards.

A Short Leash on Risk

2010 Director Compensation Review

DEPARTMENTS

8 **EDITOR'S LETTER**
Seasons of Change
by Deborah Scally

10 **FOR YOUR REVIEW**
Having a sterling reputation can drive your bank's deposit growth.

12 **TOP OF MIND**
Wavering Optimism in a Post-Reform World
The fourth quarterly Bank Executive Survey by Grant Thornton LLP shows bankers' outlook for the rest of the year took a nosedive by summer's [illegible]

[illegible]
Don't Compromise Your Card Business
Third parties can create a panoply of security challenges for card-issuing banks, and the stakes today are higher than ever.
by Chris Costanzo

54 **BOARDROOM BASICS**
Do I Need to Get My Own Lawyer?
There are times when directors and officers of a troubled financial institution should consider hiring counsel, separate and apart from bank counsel, to best protect their personal interest.
by Scott Sorrels

56 **LAW REVIEW**
Foreign Privacy Laws and the Cross-Border Transfer of Information
In an increasingly global financial world it's helpful to have some basic knowledge about the rules and regs regarding international privacy law.
by Mark D. Kotwick

64 **BOOKSHELF**
Additional reading and resources for directors.

BANK DIRECTOR
MAGAZINE

Chairman & Founder **William B. King**
Chief Executive Officer **Joan Susie**
Executive Vice President **Al Dominick**
Associate Publisher **Jack Milligan**

Editor **Deborah S. Scally**
Associate Editor **Kimberly S. Crowe**
Art Direction **Clayton Robertson, Jeff Carroll, John Robertson**

Vice President of Digital Strategy **Mika Moser**
Vice President, Director of Education **Jamie Tassa**
Director of Conferences **Laura Schield**
Director of Events **Annemarie Williams**
Director of BankBusiness.com **Kelsey Weaver**
Circulation Director **Emily McCormick**
Data and Research Manager **Dan Schuster**
Circulation Assistant **Paige Hendrickson**

EXECUTIVE OFFICE: 201 Summit View Dr., Suite 350, Brentwood, TN 37027; Telephone: 615-777-8450; Fax: 615-777-8449; bankdirector@boardmember.com; www.bankdirector.com

Bank Director (USPS 022-036), 4th Quarter 2010, volume 20, number 4. *Bank Director* is published quarterly by DirectorCorps Inc., 201 Summit View Dr., Suite 350, Brentwood, TN 37027. Periodicals Postage Paid at Brentwood, TN and at additional mailing offices.

SUBSCRIPTIONS: The subscription rate for individuals, libraries, and research institutions is $115 per year (four issues). Group rates are available. To subscribe, call 615-777-8450 or send a check, along with the name and address of the subscribers, to 201 Summit View Dr., Suite 350, Brentwood, TN 37027.

CHANGE OF ADDRESS: We will gladly change our records so that you can receive *Bank Director* at the address that is most convenient for you. Call 615-777-8450.

INDEX: *Bank Director* is indexed by FINIS (database of the Bank Marketing Association) and the ABA Banking Literature Index.

POSTMASTER: Send address changes to Bank Director, 201 Summit View Dr., Suite 350, Brentwood, TN 37027.

FOREIGN PRIVACY LAWS AND THE CROSS BORDER TRANSFER OF INFORMATION

In an increasingly global financial world, it's helpful to have some basic knowledge about the rules and regs regarding international privacy law.

by **MARK D. KOTWICK**

The cross-border transfer of information has become almost unavoidable in today's world of increasing economic globalization. Routine transfers by U.S. financial institutions of data originating from outside the United States, however, carry with them potential legal consequences under the myriad privacy laws that limit the transfer of individuals' personal data to the United States. Financial institutions, accordingly, need to be increasingly vigilant of the privacy laws of the countries with which they do business, and carefully monitor their compliance with those laws.

The transfer of information between financial institutions concerning employees, clients, customers or other individuals occurs every day with little regulatory impediment in the United States, other than discrete areas such as the collecting and use of Social Security Numbers, credit reporting, financial accounts and electronic health records. This is because, in general, U.S. law assumes that a corporation owns the data it possesses or controls. U.S. corporations thus rarely have to worry that their preservation, processing, review, or disclosure of information would violate an individual's rights to the data. Other countries, however, weigh an individual's right to privacy against the right to public access to information very differently. In particular, Europeans view information about a person as belonging to that person and consider personal data privacy a fundamental right. Their views are increasingly influencing how other countries around the globe view an individual's privacy rights.

The European Union's privacy regime

The European Union (EU) has perhaps the most comprehensive legal regime with regard to data privacy and the transfer of personal information. At the heart of these privacy laws is the EU Data Protection Directive, which went into effect in 1998 with the twin objectives of protecting individuals with respect to the processing of personal information while ensuring the free movement of that information within the EU through harmonizing different member states' privacy laws. It is important to remember that the directive itself is not a law, but rather a mandate setting out minimum standards that each of the EU's twenty-seven member states is obligated to incorporate into its own law. Consequently, actual data privacy laws vary from country to country, and when interacting with institutions in the EU, even in discrete instances, U.S. financial institutions must determine their rights and obligations under the privacy laws of each member state with which they are dealing. Then they must consider what steps have to be taken to comply with applicable laws and how to implement those steps, adopting policies and procedures to monitor their compliance with those laws.

The directive establishes a regulatory framework for the "processing" of any personal information, including the collection, storage, use, or transfer of the information. Covered data includes both private and public information, such as names, addresses, e-mail addresses, telephone numbers, marital status, financial information (such as bank account or credit card numbers), compensation, and terms of employment contracts. Additional restrictions are mandated for certain types of "sensitive" information, such as that relating to a person's race, ethnicity, political or religious beliefs, or health status. The directive places very specific (and, by American terms, often onerous) handling requirements on the processing of personal data, including notice to those whose information is being collected; limits on how the information can be processed; the rights of persons to access and correct the information collected about them; how long the information can be maintained before it must be destroyed; and measures that must be taken to protect against unauthorized access to the information. Sanctions for violating a country's privacy laws vary by member state, but include significant fines, enjoining future transfers of information by the offending party, and in some cases, criminal penalties.

The directive requires that EU member states prohibit the transfer of personal data to non-EU countries whose laws do not provide similar protections to those embodied in the directive, unless some other approved

means of assuring adequate protection of the information is in place. Notably, the EU does not consider that the United States provides "adequate" data protection under its laws. This means that a U.S. institution wanting or needing to lawfully process protected information from an EU member state must meet the requirements of the directive on a company-by-company basis.

Complying with the EU Directive

One solution to this problem was the creation of a "safe harbor" by the European Commission and the U.S. Department of Commerce, under which a U.S. company adopts a privacy program compliant with a standard set of privacy principles consistent with the Directive. A company within the safe harbor will be deemed to satisfy the requirements of the privacy laws of each of the EU member states and can freely receive data transfers from those countries. Financial institutions, including banks, credit unions, and savings and loan institutions, however, are ineligible to join the safe harbor at this time. Consequently, U.S. financial institutions have several alternatives available if they seek to import protected personal data from an EU country.

First, a U.S. institution and the exporter of the data can enter into a contract that obligates them to provide adequate safeguards for the data. The contract identifies a set of data being transferred and the purposes of the transfer, and sets out the rights and obligations of both parties in relation to the data. The contract can incorporate standard contractual clauses approved by the European Commission (amended in May of this year), which affords to individuals whose data is being exported essentially the same protections extended to them under the directive. Alternatively, the parties can negotiate an ad hoc agreement, which typically will have to incorporate comparable protections. In both cases, most EU member states require that their local authorities review and approve any proposed contract involving the transfer of personal information. In the case of either a standard contract or an ad hoc agreement, the U.S. institution assumes a contractual obligation to comply with applicable data privacy laws. Furthermore, under the standard contractual clauses, and almost necessarily in any ad hoc contract that passes muster with the local authorities, the U.S. institution will generally have to agree to joint liability with the data exporter for any damages caused to individuals resulting from the misuse of their personal information.

Second, the company exporting the data may obtain the individual's consent to the transfer of his or her personal data. A benefit of this method for the American importer of the data is that, unlike transfers pursuant to a contract, it will generally have limited obligations in relation to the imported data, and almost no liability with respect to the individual whose data is being transferred. The U.S. institution, of course, must be mindful that its exporter counterparty may be sanctioned in the event the data is misused, and thus its ability to negotiate the future transfer of information may be compromised if it misuses the transferred information.

Finally, personal data may be transferred to third countries when the transfer is necessary for the performance of a contract between the individual whose data is being transferred and the company exporting the data, or the transfer is necessary for the performance of a contract between the EU company and a U.S. institution for the benefit of that individual. This, however, is a narrow exception limited to information absolutely essential for the performance of a contract, and the transferred information can be used only for that specific purpose. In this situation, the responsibility for compliance with applicable privacy laws, and the liability for any misuse of the information, remains largely on the EU exporter of the data.

It is important to keep in mind that there are other foreign statutes governing the transfer of information separate and apart from these directive-based privacy laws, including so-called bank secrecy laws limiting the disclosure of banking and financial records, and blocking statutes purporting to limit the transfer of information in connection with foreign legal proceedings. These laws impose further and different limitations on the transfer and use of particular types of personal data and require additional consideration when encountered.

The trend of data protection laws

A collateral effect of the directive and the collective economic power of the EU is that a growing number of other countries, from Russia to Canada to Japan to Mexico (effective July of this year), have adopted, and other countries are considering, national data privacy laws closely tracking the directive. The clear trend is that privacy laws are expanding worldwide, and developing laws are likely to look like those in the EU and be significantly more stringent than those in the United States. U.S. institutions thus must be increasingly vigilant any time they are involved in the cross-border transfer of any personal data, and are likely to face mounting pressure to adopt internal privacy policies that will allow them to more easily interact and share personal information with companies outside of the United States. **|BD|**

Mark D. Kotwick is a partner in Seward & Kissel's Litigation Group and represents clients in a wide variety of complex and sensitive matters, including those involving securities litigation, banking and commercial controversies, employment law, and partnership and real estate disputes. He also regularly advises clients on employment matters, including employment contracts, restrictive covenants, reductions in force, group hirings, and other work place issues.