

**DRAFT FEDERAL PRIVACY BILL WOULD DRAMATICALLY AFFECT HOW A  
WIDE RANGE OF COMPANIES COLLECT, USE, AND DISCLOSE CERTAIN  
INFORMATION ABOUT INDIVIDUALS, BOTH ONLINE AND OFFLINE**

On May 4, 2010, Chairman Boucher (D-VA) of the House Energy and Commerce Committee's Subcommittee on Communications, Technology, and the Internet released a long-anticipated discussion draft of proposed legislation (the "Draft") that would establish broad new privacy protections for individuals and affect a wide variety of businesses that collect, use, or disclose certain information about individuals. Chairman Boucher has noted that the Draft is primarily intended to address personal information collected through an individual's use of the Internet. However, the measure is broadly drafted and would also cover businesses that collect personal information manually (*i.e.*, offline) about customers, clients, or other individuals.

In particular, the Draft would, among other things: (1) prohibit a covered business from collecting, using, or disclosing certain information about an individual without prior notice to, and consent of, the individual; (2) establish two separate kinds of consent -- opt-in and opt-out -- each of which would be applied under certain different circumstances; (3) preempt state and local laws and regulations in this area; (4) give the Federal Trade Commission (the "FTC") significant new regulatory and enforcement authority; and (5) require the FTC to adopt and impose broad new data security requirements on covered businesses, which requirements could potentially expand even some of the aggressive state laws in this area, such as the recently effective Massachusetts data security law. Finally, although various provisions in the Draft are inconsistent with existing federal law (*e.g.*, requiring *opt-in* consent before disclosing personal information to unaffiliated third parties, whereas the Gramm-Leach-Bliley Act ("GLBA") allows for an *opt-out* approach for third-party disclosures by financial institutions), it is not clear how this law would affect the GLBA, the CAN-SPAM Act, the Health Insurance Portability and Accountability Act of 1996 ("HIPAA"), and other existing federal privacy laws. A detailed summary of the Draft is provided below.

*The Draft contains ambiguous and internally inconsistent provisions. Significantly, if not clarified in certain respects, it could be read to impose onerous online and offline privacy regulations on many new companies, as well as expand the existing privacy obligations of financial services and other businesses that are already covered by existing federal and state privacy and data security laws. Chairman Boucher and the subcommittee's senior Republican, Rep. Stearns (R-FL), are seeking public comment on the draft by **June 4** and may revise the Draft based on those comments before formally introducing the measure later this year. **Companies that would be affected by the new law -- which, again, will be most companies -- should carefully review the Draft and consider submitting comments to Reps. Boucher and Stearns by June 4th.***

## SUMMARY

### Applicability and Key Definitions

1. The Draft applies to a “covered entity,” defined as a person engaged in interstate commerce that collects data containing “covered information.” However, it would not apply to any person that collects covered information from fewer than 5,000 individuals in any 12-month period and that does not collect “sensitive information.”

[NOTE: In light of the very broad definition of “covered information” described below, and the limited carve-outs from the “covered entity” definition, the new privacy protection requirements in the Draft would apply to virtually all businesses, both those that do business online and traditional brick and mortar businesses that collect, use, and disclose covered information manually/offline.]

2. “Covered information,” which is the key term, is very broadly defined and includes the following with respect to an individual:

- first name or initial and last name;
- postal or email address;
- telephone or fax number;
- unique biometric data such as a fingerprint or retina scan;
- Social Security number or other government-issued identification number;

[NOTE: The Executive Summary that accompanied the Draft incorrectly indicated that Social Security numbers and other government-issued identifiers are treated as “sensitive information” by the Draft, which would have required opt-in consent prior to the collection of these types of information.]

- financial account number or credit or debit card number, and any required security code, access code, or password necessary to permit access to an individual’s financial account;
- a “preference profile”;<sup>1</sup>
- any “unique persistent identifier,” including an Internet Protocol address, customer number, or a unique pseudonym or alias, where the identifier is used to collect, store, or identify information about a specific individual or a computer, device, or software application that is owned, used by, or associated with a particular user”;

---

<sup>1</sup> “Preference profile” is defined as a “list of information, categories of information, or preferences associated with a specific individual, *or a computer or device owned or used by a particular user* that is maintained by or relied upon by a covered entity.” (emphasis added) The highlighted language is likely intended to cover, for example, web tracking and other information typically stored by website providers in cookies saved to a computer’s browser or on its hard drive.

[**NOTE:** This component covering “unique persistent identifiers” and the “preference profile” component listed above reveal an intent to broaden the coverage of this key term beyond traditional notions of “personal information” in order to capture nonpersonal information, such as information collected in website cookies or other such technology devices, and information that may identify a computer or device (*e.g.*, IP address) rather than an individual.] or

- any other information that is collected, stored, used, or disclosed in connection with any covered information described above.<sup>2</sup>

As noted, this broad definition applies to information collected online or offline/manually. Application of the notice and consent provisions of the Draft to the offline world would be a major change for many U.S. companies.

3. “Sensitive information” means any information that is associated with covered information of an individual and relates to that individual’s (1) medical records (including medical history, mental or physical condition, or medical treatment or diagnosis by a health care professional); (2) race; (3) ethnicity; (4) religious beliefs; (5) sexual orientation; (6) financial account records and other financial information associated with a financial account, such as account balances; and (7) precise geolocation information.

[**NOTE:** The fact that the sensitive information definition covers “other financial information associated with a financial account” coupled with the fact that the “covered entity” definition applies to any entity collecting sensitive information could result in many financial institutions, such as pooled investment vehicles and their investment managers, not being excluded from the definition of a “covered entity” despite the fact that they may not collect “covered information” from 5,000 or more individuals in any 12-month period.]

### **Notice and Consent Requirements**

A covered entity is prohibited from collecting, using, or disclosing covered information from or about an individual for any purpose unless it provides the individual with a privacy notice and obtains his or her opt-out consent before collecting any of the information. When information is collected “through the Internet,” the required privacy notice must be posted “clearly and conspicuously” (undefined term) on the website through which the covered entity collects the covered information and accessible through a direct link from the Internet homepage of the covered entity. If the information is collected by any means “that does not utilize the Internet”

---

<sup>2</sup> The Draft, unlike the GLBA privacy rules, does not exclude publicly available information from the definition of covered information. Consequently, an individual’s name alone, for example, could technically trigger the Draft’s various requirements even if it can be located in a telephone book or on the Internet.

(undefined phrase, but likely means manually/offline), the notice must be provided in writing before the covered entity collects any covered information from that individual. In either case, the notice must be a “clear statement” that contains each of the required elements listed in the next section below.

1. Required Contents of Privacy Notice<sup>3</sup>

The covered entity’s privacy notice must include the following extensive information:

- the identity of the covered entity collecting the covered information;
- a description of any covered information collected, as well as how it is collected and stored;
- the specific purposes for which the covered information is collected and will be used;
- the purposes for which covered information may be disclosed and the categories of “unaffiliated parties”<sup>4</sup> that may receive such information for each purpose;
- how the covered entity may merge, link, or combine the covered information it collects with other information it acquires about the individual from unaffiliated parties;
- the period of time for which the entity will retain the information in identifiable form;
- how the information will ultimately be disposed of or rendered anonymous after the retention period;
- the choice and means the covered entity offers individuals to limit or prohibit the collection and disclosure of covered information;

[NOTE: As discussed below, different types of such “choice” mechanisms (*i.e.*, consent) would be required depending on the nature of the information and how it is to be used and/or disclosed.]

- the means by which, and the extent to which, an individual may obtain access to the covered information;
- how an individual may contact the covered entity with any inquiries or complaints regarding the entity’s handling of covered information;
- a hyperlink to or listing of the FTC’s online consumer complaint form or a toll-free telephone number for the FTC’s “Consumer Response Center”;

---

<sup>3</sup> Only a few of these content requirements are similar to those required by the GLBA rules, among them the identity of the companies collecting the information, a description of any information collected, and how such information is collected. Even the requirement in the Draft to list in all cases the categories of unaffiliated parties to which covered information is disclosed is new, as that is required by the GLBA rules *only* when no exception for such disclosure otherwise applies.

<sup>4</sup> An “unaffiliated party” is defined as “any entity that is not related by common ownership or affiliated by corporate control with a covered entity.”

- a description of the process the covered entity employs to notify individuals of material changes to its privacy notice (such process must comply with the Draft's specified form for providing notice for material changes as described below); and
- the effective date of the privacy notice.

## 2. "Opt-Out" Consent

In general, a covered entity shall be deemed to have the consent of an individual to collect and use covered information relating to that individual if the individual either gives affirmative consent for such collection and use or does not decline consent at the time the privacy notice described above is presented to the individual ("opt-out" consent), provided that the entity made a clear statement in its privacy notice informing the individual of his/her right to decline consent to such collection and use.

If the individual later declines consent, and the information collection is already underway, the entity may no longer collect covered information from the individual or use previously collected information.

In addition, a covered entity may offer the individual the opportunity to decline consent for the collection and use of only *particular* covered information, provided that the individual has been given the opportunity to decline consent for the collection and use of *all* covered information.

## 3. "Opt-In" Consent

The Draft requires that prior "express affirmative consent" ("opt-in" consent) be obtained from an individual under certain prescribed circumstances, including for:

- the collection or disclosure of sensitive information from or about an individual for any purpose;

[**NOTE:** The fact that "financial account records and other financial information associated with a financial account" is deemed by the Draft to be "sensitive information" requiring *opt-in* consent is inconsistent with the GLBA regulations, which require *opt-out* consent prior to disclosing such financial information to nonaffiliated third parties.]

- the sale, sharing, or other disclosure of covered information to an unaffiliated party;

[**NOTE:** If implemented, this provision would have a significant impact on the operations of many online and offline businesses that currently use an *opt-out* consent mechanism in connection with their disclosures of personal information to third parties for marketing purposes (assuming they offer *any* choice at all).]

- the collection *or* disclosure of covered information about all or substantially all of an individual’s “online activity” (undefined term), including across websites, for any purpose;

[NOTE: There is an exception discussed below that allows for opt-*out* consent for collection and disclosure in connection with online activity if certain specified conditions are met.]

- making a material change in the covered entity’s privacy practices governing previously collected covered information from that individual; and
- disclosing covered information for a purpose about which the individual had not previously been informed and which the individual reasonably would not expect based on the covered entity’s prior privacy notice.

[NOTE: This circumstance goes beyond existing FTC precedent; the FTC currently requires opt-in consent for material *retroactive* changes as covered by the previous bullet, whereas this bullet makes no reference to retroactive application so, unless clarified, it could be read as covering such changes even if applied only *prospectively*.]

A covered entity that has obtained express affirmative consent from an individual must provide the individual with the opportunity, without charge, to withdraw such consent at any time thereafter.

### **Exemptions**

1. Exemption for Anonymous or Aggregate Information. Nothing in the Draft prohibits a covered entity from collecting *or* disclosing “aggregate information” or covered information that has been “rendered anonymous.” “Aggregate information” is defined as “data that relates to a group or category of services or individuals, from which all information identifying an individual has been removed.” “Render anonymous” means “to remove or obscure covered information such that the remaining information does not identify, and there is no reasonable basis to believe that the information can be used to identify (1) the specific individual to whom such covered information relates; or (2) a computer or device owned or used by a particular user.”

[NOTE: It is not clear what is intended by the second prong of the “render anonymous” definition; it could be read, for example, to indicate that if cookie data is involved that is linked to a particular *computer*, the information is not anonymous, even though no particular *individual* could be identified.]

2. Exemption from Notice Requirements. The Draft’s privacy notice requirements described above do not apply to covered information collected by any means that does not utilize the Internet (*i.e.*, offline data collected manually) and *either* (1) is collected for a “transactional purpose” or an “operational purpose”<sup>5</sup> or (2) consists solely of an individual’s name, address, telephone number, fax, and/or email address, and is part of a “first party transaction.”<sup>6</sup>

[NOTE: There is no comparable exemption from the privacy *notice* requirement for covered information collected *online*.]

3. Exemptions from Consent Requirements

*Transactional or Operational Purpose.* Prior consent is *not* required for the collection, use, or disclosure of covered information for an “operational purpose” or a “transactional purpose” as defined above (*e.g.*, Web logs or session cookies necessary for the functioning of the website, for the general servicing of an investor account, etc.). However, the consent requirement shall apply to the collection of covered information for marketing, advertising, or selling purposes, or any use or disclosure of covered information to an unaffiliated party for such purposes.

[NOTE 1: The exemption in Section 3(a)(5)(B) of the Draft needs clarification. Currently it states that the consent requirements “of this subsection” (which mandate *opt-out* consent for the *collection and use* of covered information) “shall apply” to the collection, use, *and disclosure* of covered information to any unaffiliated party for marketing, advertising, or selling purposes. This appears to require *opt-out* consent in

---

<sup>5</sup> “Transactional purpose” is defined simply as “a purpose necessary for effecting, administering, or enforcing a transaction between a covered entity and an individual.” “Operational purpose” is defined as “a purpose reasonably necessary for the operation of the covered entity,” including the following: “(1) providing, operating, or improving a product or service used, requested, or authorized by an individual; (2) detecting, preventing, or acting against actual or reasonably suspected threats to the covered entity’s product or service, including security attacks, unauthorized transactions, and fraud; (3) analyzing data related to use of the product or service for purposes of optimizing or improving the covered entity’s products, services, or operations; (4) carrying out an employment relationship with an individual; (5) disclosing covered information based on a good faith belief that such disclosure is necessary to comply with a federal, state, or local law, rule, or other applicable legal requirement, including disclosures pursuant to a court order, subpoena, summons, or other properly executed compulsory process; and (6) disclosing covered information to a parent company of, controlled subsidiary of, or affiliate of the covered entity, or other covered entity under common control with the covered entity where the parent, subsidiary, affiliate, or other covered entity operates under a common or substantially similar set of internal policies and procedures as the covered entity, and the policies and procedures include adherence to the covered entity’s privacy policies as set forth in its privacy notice.” Operational purpose does *not* include the use of covered information for marketing, advertising, or sales purposes, or any use of or disclosure of covered information to an unaffiliated party for such purposes.

<sup>6</sup> A “first party transaction” is an “interaction between an entity that collects covered information when an individual visits that entity’s website or place of business and the individual from whom covered information is collected.”

connection with the disclosure of covered information to unaffiliated parties for marketing. By contrast, Section 3(b) of the Draft states that disclosure of covered information to unaffiliated parties requires *opt-in* consent, and makes no mention of marketing purposes or an exception for transactional or operational purposes. Presumably the intent of the Draft is to require *opt-in* consent for the disclosure of covered information to unaffiliated parties *except* where such disclosure is for a transactional or operational purpose in which case *no consent* is required (which is how this point is summarized in the “Executive Summary” that was released along with the Draft). In any event, changes to Section 3(a)(5)(B) and/or Section 3(b) are needed to make the intended approach clear.]

[**NOTE 2:** Due to the fact that sensitive information is so broadly defined to include “other financial information associated with a financial account,” the Draft could be read (depending on the interpretation of the “Effect on Other Laws” section discussed below) to require certain financial institutions to provide a notice and obtain an opt-in consent even if they are exempt, under the transactional or operational purposes test, from the notice and opt-out consent requirements for collecting, using, or disclosing covered information.]

*Certain Information Sharing with Service Providers.* Opt-in consent is not required for the disclosure of covered information to an unaffiliated service provider<sup>7</sup> for purposes of executing a “first party transaction” if: (1) the covered entity has obtained opt-out consent for the collection of such covered information as described above; and (2) the service provider agrees to use such covered information solely for the purpose of providing an agreed-upon service to a covered entity and not to disclose the covered information to any other person.

[**NOTE:** It is unclear under the Draft whether this service provider exemption and its associated restrictions apply if a covered entity is exempt, under the transactional or operational purpose test described above, from the notice and opt-out consent requirements for collecting, using, or disclosing covered information. It is also unclear whether by the phrase “to any other person” the Draft means to prevent service providers from disclosing covered information to their affiliates in connection with their provision of service to the covered entity.]

---

<sup>7</sup> A “service provider” is defined as “an entity that collects, maintains, processes, stores, or otherwise handles covered information on behalf of a covered entity, including, for purposes of serving as a data processing center, providing customer support, serving advertisements to the website of the covered entity, maintaining the covered entity’s records, or performing other administrative support functions for the covered entity.”

*Online Tracking for Behavioral Advertising.* The Draft would create an exception to the requirement for *opt-in* consent to collect, use, or disclose covered information in connection with an individual's online activity (the focus is on the use of such information for targeted web advertising) where the following four conditions are met:

(1) the covered entity provides individuals with the ability to opt out of the collection, use, and disclosure of covered information by the covered entity using a readily accessible opt-out mechanism, whereby the opt-out choice of the individual is preserved and protected from incidental or accidental deletion, including by (A) interactions on the covered entity's website or a website where the preference profile is being used; (B) a toll-free phone number; or (C) a letter to an address provided by the covered entity;

[NOTE: The above language requiring the opt-out mechanism to be "preserved and protected from incidental or accidental deletion" is directed at the fact that many opt-out choice mechanisms in use today are cookie-based and can be inadvertently undone if a user deletes his or her cookies. Thus, were the Draft to be enacted, it would have a significant impact on how companies implement opt-out choices to consumers.]

(2) the covered entity deletes or renders anonymous any covered information within 18 months;

(3) the covered entity includes the placement of a symbol or seal in a prominent location on the website of the covered entity and on or near any advertisements delivered by the covered entity based on the preference profile of an individual that enables an individual to connect to additional information that—

(A) describes the practices used by the covered entity or by an "advertisement network"<sup>8</sup> in which the covered entity participates to create a preference profile that led to the delivery of the advertisement using an individual's preference profile, including the information, categories of information, or list of preferences associated with the individual that may have led to the delivery of the advertisement to that individual; and

(B) allows individuals to review and modify, or completely opt out of having, a preference profile created and maintained by a covered entity or by an advertisement network in which the covered entity participates; and

(4) an advertisement network to which a covered entity discloses covered information under this subsection does not disclose such covered information to any other entity without the express affirmative consent of the individual to whom the covered information relates.

---

<sup>8</sup> "Advertisement network" means "an entity that provides advertisements to participating websites on the basis of individuals' activity across some or all of those websites."

### **Consumer Education Campaign by the FTC**

The FTC is required to conduct a campaign to educate the public regarding opt-out and opt-in consent rights under the Draft.

### **Accuracy and Data Security of Covered Information**

A covered entity would be required to establish reasonable procedures for assuring that the covered information it collects is accurate.

In addition, covered entities or service providers that collect covered information for any purpose must “establish, implement, and maintain appropriate administrative, technical, and physical safeguards” that the FTC determines are necessary to: (1) ensure the security, integrity, and confidentiality of such information; (2) protect against anticipated threats or hazards to the security or integrity of such information; (3) protect against unauthorized access to and loss, misuse, alteration, or destruction of such information; and (4) in the event of a security breach, determine the scope of the breach, make every reasonable attempt to prevent further unauthorized access to the affected covered information, and restore reasonable integrity to the affected covered information. The Draft does not include any breach notification requirements, which, of course, are already covered by many state laws and a few federal laws, as well as other pending federal legislation.

In developing standards to implement this section of the Draft, the FTC must consider the size and complexity of a covered entity, the nature and scope of the activities of a covered entity, the sensitivity of the covered information, the current state of the art in administrative, technical, and physical safeguards for protecting information, and the cost of implementing such safeguards.

[NOTE: Given the broad definition of “covered information,” this provision could dramatically expand current law on data security. For example, even the Massachusetts data security law, which became effective on March 1, 2010, and which many cite as the most onerous of its kind, contains a definition of personal information that targets a narrower set of personal information, such as name *plus* Social Security number, or name *plus* credit card number in combination with access code, etc., not simply name *or* email address as is the case with the Draft.]

### **Use of Location-Based Information**

The Draft would, in general, prohibit any provider of a product or service that uses “location-based information” from disclosing such information concerning the user of such a product or service without the user’s “express opt-in consent.”

[NOTE: The phrase “express opt-in consent” used in this provision of the Draft is different from the phrase “express affirmative consent” in other provisions. These terms likely are intended to mean the same thing, though this should be clarified.]

### **Enforcement**

1. **FTC.** The Draft authorizes the FTC to enforce the new provisions and to issue regulations implementing its requirements (but such regulations may not require the deployment or use of any specific products or software or hardware technologies). A violation would be considered an unfair or deceptive act or practice within the meaning of the Federal Trade Commission Act. Solely for purposes of the Draft, the FTC may also enforce the provisions of the Draft against telephone companies and other common carriers that are currently exempt from FTC jurisdiction.

2. **State Attorneys General/Agencies.** In any case in which a state attorney general or agency having consumer protection responsibility believes that an interest of the residents of that state has been or is being threatened or adversely affected by any person who violates the Draft, the state attorney general or agency may bring a civil action on behalf of the residents of the state in a U.S. district court to enjoin such action, compel compliance with the Draft, obtain damages or other compensation, or seek any other appropriate relief. The state must provide the FTC with notice of any such action, and the FTC may intervene, be heard, and file petitions for appeal. No state attorney general or agency may bring such an action if the FTC already has a pending civil action for a violation of the Draft. Nothing in the Draft affects the ability of a state attorney general to conduct investigations, administer oaths or affirmations, or compel testimony or the production of evidence.

3. **No Private Right of Action.** The Draft would not create a private right of action relating to any act or practice covered by the Draft in any state court or under state law, including a pendant state claim to an action under federal law.

### **Preemption of State Laws**

The Draft supersedes any provision of a statute, regulation, or rule of a state or political subdivision of a state, that “includes requirements for the collection, use, or disclosure of covered information.”

[NOTE: It is not clear how expansively this provision would be interpreted to apply. For example, does it preempt the state laws in California and Vermont that to date have exceeded the requirements for notice and consent required by the GLBA? Does it preempt state data *security* laws like the recently effective Massachusetts law?]

### **Effect on Other Laws**

The Draft states that “except as provided expressly in this Act,” the new law “shall have no effect” on activities covered by the following specifically enumerated federal laws: (1) Title V of the GLBA, (2) the Fair Credit Reporting Act, (3) HIPAA, (4) the Children’s Online Privacy Protection Act of 1998 (“COPPA”), (5) the Communications Act of 1934; (6) the CAN-SPAM Act; and (7) Part C of title XI of the Social Security Act. In addition, the Draft states that nothing contained in the Draft shall be construed to limit the FTC’s authority under any other law.

[NOTE: It is not at all clear what is meant by the prefatory phrase “except as provided expressly in this Act.” If the intent is to leave those laws intact, it is not clear how they would interact with this new law. To cite one example, the GLBA requires notice and opt-out consent in order to disclose nonpublic personal information to nonaffiliated third parties for marketing purposes, whereas the Draft requires opt-in consent for such disclosure. This is an area that must be clarified to avoid creating overlapping and/or inconsistent regulation and much confusion in the financial services and other industries.]

**Federal Communications Commission (“FCC”) Report to Congress**

Within one year of enactment, the FCC must provide a report to Congress that describes (1) all provisions of U.S. communications law that address subscriber privacy; and (2) how these provisions may be harmonized with the provisions of the Draft to create a consistent regulatory regime for covered entities and individuals.

**Effective Date**

Unless otherwise specified, the Draft shall apply to the collection, use, or disclosure of, and other actions with respect to, covered information that occurs one year after enactment.

**IMPLICATIONS**

As indicated above, the Draft is a very broad piece of legislation that, if enacted as is, could have a significant impact on a wide cross-section of companies across all industries, including the possibility of creating new, and more onerous, burdens and regulations for financial services and other industries that are already subject to various privacy and data security requirements. However, in view of the congressional recess scheduled for the month of August, Congress’s target adjournment date of October 8, the absence of a companion Senate bill, and an already crowded legislative agenda, there is relatively little time left for Congress to act on the Draft during this session. Rather, Reps. Boucher and Stearns are likely to use the remainder of the session to evaluate the responses to the Draft from affected constituencies, potentially make some revisions and even release a bill, but such bill would likely serve as the foundation for consideration in the next Congress. Still, companies should carefully review the Draft and ***consider filing comments on it by June 4, 2010***, in order to minimize any negative impacts on their business.

\*\*\*\*\*

If you have any questions regarding the discussion draft, please contact Frank Buono (202-303-1104, fbuono@willkie.com), Pamela Strauss (202-303-1154, pstrauss@willkie.com), Barbara Block (202-303-1178, bblock@willkie.com), Melissa Troiano (202-303-1183, mtroiano@willkie.com), Marc J. Lederer (212-728-8624, mlederer@willkie.com), or the Willkie attorney with whom you regularly work.

Willkie Farr & Gallagher LLP is headquartered at 787 Seventh Avenue, New York, NY 10019-6099 and has an office located at 1875 K Street, NW, Washington, DC 20006-1238. Our New York telephone number is (212) 728-8000 and our facsimile number is (212) 728-8111. Our Washington, DC telephone number is (202) 303-1000 and our facsimile number is (202) 303-2000. Our website is located at [www.willkie.com](http://www.willkie.com).

May 20, 2010

Copyright © 2010 by Willkie Farr & Gallagher LLP.

All Rights Reserved. This memorandum may not be reproduced or disseminated in any form without the express permission of Willkie Farr & Gallagher LLP. This memorandum is provided for news and information purposes only and does not constitute legal advice or an invitation to an attorney-client relationship. While every effort has been made to ensure the accuracy of the information contained herein, Willkie Farr & Gallagher LLP does not guarantee such accuracy and cannot be held liable for any errors in or any reliance upon this information. Under New York's Code of Professional Responsibility, this material may constitute attorney advertising. Prior results do not guarantee a similar outcome.