THE UNITING AND STRENGTHENING AMERICA BY PROVIDING APPROPRIATE TOOLS REQUIRED TO INTERCEPT AND OBSTRUCT TERRORISM ("USA PATRIOT ACT") ACT OF 2001

SIMPSON THACHER & BARTLETT LLP

NOVEMBER 12, 2001

On October 26, 2001, President Bush signed the Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism (the "USA Patriot Act" or the "Act") Act of 2001, a sprawling anti-terrorism statute granting federal law enforcement agencies increased powers to prevent, investigate and prosecute terrorist activity and money laundering by individuals, organizations and foreign governments. The Act strengthens an array of existing law enforcement statutes, including the Bank Secrecy Act, the Money Laundering Control Act of 1986, the Racketeer Influenced and Corrupt Organizations Act ("RICO") and the Foreign Intelligence Surveillance Act of 1978, and adopts many new counter-terrorism measures. Bearing marks of compromise, concession and hurried drafting, however, the Act is not a model of legislative clarity.

In the wake of September 11, sustained efforts by the financial services industry to limit governmental constraints and disclosure obligations yielded to overwhelming public demand for immediate measures to extirpate transnational terrorist activities. Recognizing that identification and seizure of financial assets used to fund terrorist activities must be a cornerstone of anti-terrorist initiatives, the Act includes far-reaching provisions affecting banks and other financial institutions. Of particular interest to financial institutions is Title III of the Act – the International Money Laundering Abatement and Anti-terrorist Financing Act of 2001 – which imposes a host of information collection and disclosure obligations on banks and other financial institutions, all of which are animated by the expectation that increased transparency in financial transactions will assist law enforcement in eliminating the financing of global terrorism. Title III will not terminate before 2005, and then only if Congress enacts a joint resolution providing for termination.

This memorandum summarizes the provisions of the Act most likely to affect a broad segment of the business community.

DEFINITIONS OF "FINANCIAL INSTITUTIONS" AND "MONEY LAUNDERING"

"Financial institutions" are most directly affected by the anti-money laundering provisions of the Act. The Act incorporates and expands the already broad definition of "financial institution" contained in the Bank Secrecy Act, 31 U.S.C. § 5312 (a)(2), which encompasses, *inter alia*, insured banks, commercial banks and trust companies, brokers and

dealers of securities or commodities, investment bankers, investment companies, insurance companies and money handling institutions such as travel agencies, casinos and the United States Postal Service. Section 321 of the Act amends 31 U.S.C. § 5312 (a)(2) to add (i) banks operating outside the United States, (ii) credit unions, (iii) futures commission merchants, (iv) commodity trading advisors, and (v) registered commodity pool operators to the definition of financial institution for purposes of the Bank Secrecy Act.

The centrality of "money laundering" to the Act's financial provisions warrants a short description of what constitutes money laundering. Money laundering is the process by which one conceals the existence, illegal source or illegal application of income, and disguises that income to make it appear legitimate. Generally, in the Money Laundering Control Act of 1986 (18 U.S.C. §§ 1956-57), Congress prohibited financial transactions involving proceeds of "specified unlawful activity": (i) with the "intent to promote" the specified unlawful activity; (ii) knowing that the transaction is designed to conceal the "nature, the location, the source, the ownership, or the control" of the funds; or (iii) with the intent to "avoid a transaction reporting requirement [such as under the Bank Secrecy Act]." The Money Laundering Control Act defines a myriad of specific acts or activities that constitute discrete federal or state law offenses as "specified unlawful activity." Section 315 of the Act adopts and expands the Money Laundering Control Act's list of "specified unlawful activities" to include foreign corruption offenses, certain United States smuggling and export control offenses, certain customs and firearms offenses, certain computer fraud offenses, and felony violations of the Foreign Agents Registration Act of 1938. Notably, not all of these proscribed activities necessarily relate to terrorism.

ESTABLISHMENT OF GENERAL ANTI-MONEY LAUNDERING PROGRAM

Concluding that money laundering constitutes a staggering 2-5% of global gross domestic product and that limited financial transparency has thwarted efforts to root out terrorist funding, the Act requires financial institutions to adopt broad anti-money laundering measures. Within 180 days of enactment, financial institutions must at a minimum (i) develop internal policies and controls calculated to detect and disclose money laundering to law enforcement; (ii) designate an officer to monitor compliance with the policies; (iii) conduct an ongoing employee training program; and (iv) implement an independent audit function to test the programs. Before the 180-day period expires, the Secretary of the Treasury ("Secretary") will prescribe regulations that will reflect the extent to which the anti-money laundering measures are commensurate with the size, location and activities of affected financial institutions.

Section 319 of the Act amends the Bank Secrecy Act (new subsection (k) to 31 U.S.C. § 5318) to require U.S. financial institutions to reply to a request for information from a U.S. regulator relating to anti-money laundering compliance within 120 hours of receipt of such a request. Compliance entails making available information and account documentation for any account opened or managed in the United States by a covered financial institution.

Section 312 of the Act further amends the Bank Secrecy Act to impose due diligence requirements on domestic financial institutions relating to certain private banking accounts and correspondent accounts. These due diligence requirements, described immediately below, take effect 270 days after enactment. Section 352 of the Act requires the Secretary to issue regulations further delineating the due diligence requirements within 180 days of enactment, but the requirements take effect whether or not such regulations are issued.

MINIMUM DUE DILIGENCE FOR PRIVATE BANKING ACCOUNTS

The Act defines a "private banking account" as one with at least $1 million in assets and which is managed by an agent of a financial institution acting as liaison between the financial institution and the direct or beneficial account owner. Any financial institution that establishes, maintains, administers or manages a private banking account in the United States for a non-United States person (including a foreign individual visiting the United States and a representative of a non-United States person) must establish due diligence procedures "reasonably designed to detect and report instances of money laundering through those accounts." The due diligence policies must at a minimum ensure that domestic financial institutions take reasonable steps to:

- identify the nominal and beneficial owners and sources of funds deposited into such accounts;
- conduct enhanced scrutiny of any account requested or maintained by, or on behalf of, a senior foreign political figure or his/her immediate family members or close associates; and
- report any suspicious activity or that which may involve proceeds of foreign corruption to the Secretary's designee.

MINIMUM DUE DILIGENCE FOR CORRESPONDENT ACCOUNTS

The Act defines a correspondent account as "an account established to receive deposits from, make payments on behalf of a foreign financial institution, or handle other financial transactions related to such institution." The Act identifies correspondent banking facilities as a banking mechanism particularly vulnerable to manipulation by foreign banks to permit the laundering of funds by concealing the identity of transactional real parties in interest. Accordingly, section 312 of the Act imposes enhanced due diligence requirements as to correspondent accounts maintained by foreign banks operating either under offshore banking licenses or banking licenses issued by a foreign country that has been designated (a) as non-cooperative with international money laundering principles by an international body, with the concurrence in such designation by the United States representative to that body, or (b) by the Secretary as warranting "special measures" discussed in the next section herein. As to correspondent accounts fitting these criteria, within 270 days of enactment domestic financial institutions must:

- for any such foreign bank (the shares of which are not publicly traded) requesting a correspondent account, ascertain the identity of each of the owners of the foreign bank, and the nature and extent of the ownership interest of each such owner;

- conduct enhanced scrutiny of such accounts to guard against money laundering and report any suspicious transactions under the terms of 31 U.S.C. § 5318(g) to the Secretary's designee; and

- ascertain whether any foreign bank in turn provides correspondent accounts to third party foreign banks; if so the U.S. financial institution must ascertain the identity of those third party foreign banks and related due diligence information required under the general rules of 31 U.S.C. § 5318(i)(1).

The Secretary or the Attorney General may issue a summons or subpoena to any foreign bank that maintains a correspondent account in the United States and request information concerning such account, including information maintained outside the United States. A summons or subpoena may be served in the United States on a representative of the foreign bank, or in a foreign country pursuant to any applicable international agreement. Within ten business days of receipt of written notice from the Secretary or the Attorney General that a foreign bank has failed to comply with a subpoena or summons and subject to a $10,000 civil penalty, a domestic financial institution must sever any correspondent relationship with the non-complying foreign bank. The Act confers immunity on any domestic financial institution that terminates a correspondent relationship under this provision.

Further, pursuant to section 319, the Bank Secrecy Act (31 U.S.C. § 5318(k)) is amended to require any financial institution that maintains a correspondent account in the United States for a foreign bank to maintain records identifying the owners of the foreign bank and the name and address of a person who resides in the United States who is authorized to accept service regarding the correspondent account. The covered financial institution must provide this information to a federal law enforcement officer within seven days of receiving the request. Financial institutions have sixty days from enactment to comply with the amendments contained in section 5318(k).

"PRIMARY MONEY LAUNDERING CONCERNS"

Section 311 of the Act amends the Bank Secrecy Act by authorizing the Secretary to designate an extra-territorial jurisdiction, a financial institution operating outside the United States or even specific bank accounts a "primary money laundering concern." The designation of an entity as a primary money laundering concern empowers the Secretary (in consultation with specified federal regulators) to require domestic financial institutions to take one or more of five enumerated "special measures" with respect to such foreign entity as follows:

- requiring additional record keeping and reporting by any domestic financial institution or financial agency concerning transactions entered into by the entities identified;

- requiring any domestic financial institution or financial agency to take reasonable and practicable steps to obtain and retain information concerning foreign beneficial owners of any account opened in the United States by a foreign person (other than foreign entities whose shares are subject to public reporting requirements or are listed and traded on a regulated exchange or foreign market);

- requiring any domestic financial institution or financial agency that opens or maintains a payable-through account for a foreign financial institution implicating money laundering concerns, or a payable-through account through which transactions of concern may be conducted, to identify each customer who uses the account or whose transactions are routed through the account, and to obtain information about such customer comparable to that which it obtains in the ordinary course of business with respect to customers residing in the United States;

- requiring any domestic financial institution or financial agency that opens or maintains a correspondent account for a foreign financial institution implicating money laundering concerns, or opens or maintains a correspondent account through which transactions of concern may be conducted, to identify each customer who uses the account or whose transactions are routed through the account, and to obtain information about such customer comparable to that which it obtains in the ordinary course of business with respect to customers residing in the United States; or

- after consultation with the Secretary of State, Attorney General and Federal Reserve Chairman, the Secretary may prohibit or restrict the opening or maintaining of a correspondent account or payable-through account by any domestic financial institution or financial agency on behalf of a specified foreign banking institution.

The first four "special measures" may be imposed for up to 120 days without a Treasury regulation; the fifth measure may not be imposed without a Treasury regulation.

SHELL BANKS

Section 313 of the Act prohibits financial institutions from establishing, administering or managing correspondent accounts for foreign shell banks (banks having no physical presence in any country). In addition, financial institutions must take reasonable steps to ensure that they are not used by foreign banks to indirectly provide banking services for foreign shell banks.

This provision permits a financial institution to provide a correspondent account to a foreign bank that is affiliated with a depository institution, credit union, or foreign bank that maintains a physical presence in a foreign country or in the United States, and which is subject to banking authority in the country regulating the affiliated entity. The shell bank provisions take effect 60 days after the Act's October 26 enactment.

CONCENTRATION ACCOUNTS

Concentration accounts are a recognized commercial banking mechanism used to commingle related funds temporarily in one place pending disbursement or the transfer of funds into individual client accounts. Parent companies and their subsidiaries, for example, frequently use concentration accounts. Finding that concentration accounts have been used to launder funds, section 325 of the Act authorizes the Secretary to issue regulations to bar the use of concentration accounts to move client funds anonymously, without documentation linking particular funds to their true owners. The regulations will:

- prohibit financial institutions from allowing clients to direct transactions that move funds into, out of or through concentration accounts;
- prohibit financial institutions and their employees from informing customers of the existence of the financial institution's concentration accounts; and
- require financial institutions to establish written procedures ensuring that whenever a transaction involving a concentration account commingles funds belonging to one or more customers, the identity of and specific amount belonging to each customer is documented.

COOPERATION AND INFORMATION SHARING

Section 314 of the Act requires the Secretary within 120 days of enactment to issue regulations designed to encourage law enforcement and regulatory authorities to share information with financial institutions regarding "individuals, entities and organizations engaged in or reasonably suspected based on credible evidence of engaging in terrorist acts or money laundering activities." The regulations will require financial institutions to designate contact-people responsible for receiving information from the authorities and thereafter monitoring accounts of entities identified as suspicious. The receipt of information by a financial institution does not relieve or modify its obligations to other persons or accounts, and the information may only be used for the purposes of identifying and reporting on activities that may involve terrorist acts or money laundering activities. This section also allows (upon notice to the Secretary) financial institutions to exchange information regarding suspected terrorist or money laundering activities, and provides complete immunity to any financial institution that discloses customer information for purposes of reporting terrorist or money-laundering activity. Compliance with this provision will not violate the privacy provisions of Title V of the Gramm-Leech-Bliley Act. The Secretary is required to publish a report, at least

semiannually, detailing patterns of suspicious activity and other investigative insights, and distribute the report to financial institutions.

Section 361 adds section 310 to subchapter I of chapter 3 of the Bank Secrecy Act, to make the Financial Crimes Enforcement Network ("FinCEN") a bureau within the Department of the Treasury, to list the duties of FinCEN's Director and to require the Secretary to establish operating procedures for the government-wide data access service and communications center maintained by FinCEN. The Secretary will establish, within nine months of enactment, a secure network through FinCEN that will allow financial institutions to file suspicious activity reports and provide such institutions with information regarding suspicious activities warranting special scrutiny.

CUSTOMER IDENTIFICATION AND ACCOUNT OPENING

Section 326 of the Act adds a new subsection (l) to 31 U.S.C. § 5318 to require the Secretary within one year to prescribe minimum standards for financial institutions regarding the identification of customers that must be satisfied in connection with the opening of an account. The regulations will require adoption of reasonable procedures for:

- verification of customer identity when opening an account;
- maintenance of records of customer information used for identity verification; and
- consultation of lists of known or suspected terrorists provided to the financial institution by any government agency to facilitate determining whether a person seeking to open an account is a known or suspected terrorist.

The Secretary is required to submit recommendations to Congress, within six months of the date of enactment, of the most effective ways to compel foreign nationals to provide domestic financial institutions and agencies with accurate customer identity information (comparable to the identity information required of United States nationals) and to obtain an identification number akin to a Social Security number or tax identification number before opening an account.

BROKER-DEALER AND COMMODITY-RELATED SUSPICIOUS ACTIVITY REPORTS

Section 356 of the Act expands the requirement presently imposed on banks to submit "suspicious activity reports" to a variety of additional businesses. Under the Act, brokers and dealers registered under the Securities Exchange Act of 1934, futures commission merchants, commodity trading advisers and commodity pool operators registered under the Commodity Exchange Act now must submit suspicious activity reports to both law enforcement and intelligence agencies. The Secretary, after consulting the SEC, the Board of Governors of the

Federal Reserve System and the Commodity Futures Trading Commission, will publish proposed implementing regulations before January 1, 2002.

While broker-dealers that are subsidiaries of bank holding companies are already subject to reporting requirements, extending reporting obligations to this broader segment of the investment community will create time and resource intensive obligations, warranting prompt review and commentary by affected groups on proposed regulations. A preview of what may trigger the obligation to file a suspicious activity report may be drawn from the SAR requirements currently imposed on banks. A bank must file an SAR with "appropriate Federal law enforcement agencies and the Department of Treasury" when it detects a known or suspected (i) federal criminal violation involving a bank employee and in which the bank was a victim or used to facilitate the violation; (ii) violation conducted through the bank and involving at least $5,000, if the bank has a substantial basis for identifying a suspect; (iii) violation conducted through the bank and involving at least $25,000 even if the bank has no substantial basis for identifying a suspect; and (iv) transaction involving at least $5,000 if the bank suspects that the transaction involves funds derived from illegal activities, is designed to evade the Bank Secrecy Act or the transaction has no business or apparent lawful purpose. Currently, SARs must be filed confidentially and within 30 days of the initial detection of the possible violation, and the bank's board of directors must be notified of the filing.

Section 356(c) requires the Secretary of the Treasury, the SEC and Federal Reserve Board to submit jointly to Congress, within one year of the date of enactment, recommendations for regulations to apply the Bank Secrecy Act's reporting and record keeping provisions to both registered and unregistered investment companies, as well as recommendations as to whether the Secretary should promulgate regulations treating personal holding companies as financial institutions that must disclose their beneficial owners when opening accounts or initiating funds transfers at any domestic financial institution.

NON-DISCLOSURE OF REPORTING AND GENERAL IMMUNITY PROVISION

The Act expressly forbids any financial institution or its representative who reports a suspicious transaction to a government agency from notifying any person involved in the transaction that the transaction has been reported, except in limited employment-related matters. Section 351 of the Act amends the Bank Secrecy Act's safe harbor provision, and confers blanket immunity on any financial institution or employee or agent of such institution that makes a voluntary disclosure, or a disclosure pursuant to this provision or any other authority, of a possible violation of law or regulation to a government agency.

LONG ARM JURISDICTION

Section 317 of the Act confers "long arm" jurisdiction in United States district courts over foreign defendants in money laundering prosecutions. Any foreign person, including any financial institution, is subject to this jurisdiction so long as service of process upon the foreign

person is made under the Federal Rules of Civil Procedure or under the laws of the country in which the foreign person is found and one of the following conditions is met:

- the foreign person commits a money laundering offense involving a transaction that occurs in whole or in part in the United States;
- the foreign person converts assets ordered forfeited by a U.S. court; or
- the foreign person is a financial institution that maintains a bank account at a domestic financial institution.

District courts may issue pre-trial restraining orders or take other actions necessary to preserve property held by the defendants in the United States in order to secure ultimate judgments.

FORFEITURE OF FUNDS IN INTERBANK ACCOUNTS

For the purpose of forfeiture, section 319 of the Act amends 18 U.S.C. § 981 to treat funds deposited in a foreign bank that has an interbank account in the United States with a covered financial institution as having been deposited into the interbank account in the United States. The Attorney General may suspend or terminate a forfeiture where a conflict a law exists between the laws of the United States and the jurisdiction in which the foreign bank is located with respect to liabilities arising from the seizure of the funds. If a forfeiture action is brought against seized funds, the owner of the funds may contest the action but the Government need not establish that the funds are directly traceable to the funds deposited in the foreign bank.

CURRENCY TRANSACTIONS

The Act requires any person who receives more than $10,000 in coins or currency in a single transaction (or in two or more related transactions) in the course of his or her trade or business to file a report with respect to such transaction with the Financial Crimes Enforcement Network. This requirement does not apply to amounts received in a transaction reported under 31 U.S.C. § 5313 or to transactions that took place entirely outside the United States. The Secretary will promulgate regulations to implement this reporting requirement within six months of enactment.

SEIZURE OF PROPERTY

Section 215 of the Act amends the Foreign Intelligence Surveillance Act of 1978 to allow the FBI to obtain a court order for the production of "any tangible things (including books, records, papers, documents and other items)" in relation to "an investigation to protect against international terrorism or clandestine intelligence activities." Significantly, the entity producing such "tangible things" may not disclose to anyone that the FBI obtained these items pursuant to a Foreign Intelligence Surveillance Act order. Good faith compliance with an order secured by the FBI is protected by blanket immunity.

Similarly, section 106 of the Act amends the International Emergency Powers Act to allow the President to respond to an attack by a foreign country or foreign nationals or ongoing armed hostilities by confiscating any property within the United States' jurisdiction of "any foreign person, foreign organization, or foreign country that he determines has planned, authorized, aided, or engaged" in the hostilities or attacks.

IMPLICATIONS FOR THE RACKETEER INFLUENCED AND CORRUPT ORGANIZATIONS STATUTE (RICO)

The RICO statute prohibits any person, including corporations, from (1) using income derived from a pattern of racketeering activity to acquire an interest in any enterprise engaged in interstate or foreign commerce, (2) acquiring an interest in any such enterprise through a pattern of racketeering activity or (3) conducting the affairs of any such enterprise through a pattern of racketeering activity. 18 U.S.C. § 1961 defines "racketeering activity" to include, among other activities, any act that is indictable under the Money Laundering Control Act of 1986 (18 U.S.C. §§ 1956-57). Section 315 of the Act expands the Money Laundering Control Act's definition of "specified unlawful activities," to include bribery of a public official and certain smuggling and export violations, including smuggling violations involving (i) any item on the United States Munitions List established under section 38 of the Arms Export Control Act (22 U.S.C. § 2778) or (ii) any item controlled under the Export Administration Regulations (15 C.F.R. Parts 730-774). While an exhaustive list of the items and prohibitions encompassed is not practicable here, the Export Administration Regulations set forth voluminous lists of products (ranging from computers and software to uranium) prohibited from export to proscribed countries. Violations of these smuggling and export control regulations are now "specified unlawful activities," which may support a money laundering RICO predicate act.

Section 813 also affects RICO. Section 813 adds terrorism — as defined in 18 U.S.C. § 2332b's definition of "federal crime of terrorism" — as "racketeering activity" under 18 U.S.C. § 1961. Because providing material support to terrorists and to terrorist organizations are federal crimes of terrorism under section 2332b, they are also "racketeering activities" for purposes of RICO.

INTERNET SERVICE PROVIDERS (ISP), TELECOMMUNICATIONS AND CONSUMER REPORTING AGENCIES

Generally, 18 U.S.C. § 2702 prohibits an ISP from disclosing communications transmitted or stored on its systems. Section 212 of the Act reiterates this rule by prohibiting a "provider of remote computer service or electronic communication service to the public" from voluntarily providing records or information about a customer to the government. However, this section adds an exception allowing a provider to voluntarily disclose to a governmental entity the contents of a communication and/or the customer record if the provider "reasonably believes that an emergency involving immediate danger of death or serious physical injury" requires such disclosure. Moreover, section 212 amends 18 U.S.C. § 2703 to authorize law enforcement to demand disclosure of a customer's record or other subscriber/customer information (other

than the contents of electronic communications) from any provider of remote computer service or electronic communication service to the public. The amendments effected by section 212 terminate on December 31, 2005.

Section 216 expands permissible surveillance techniques by allowing, in addition to pen registers, "trap and trace devices" focused on capturing routing and addressing information for electronic communications. In other words, while existing law allowed pen registers which capture the phone number dialed from a targeted telephone, the amendment authorizes law enforcement to use devices that record the Internet web-pages accessed by a targeted internet user. Court authorization for these surveillance activities does not require probable cause but rather a simple certification that the information sought is relevant to an ongoing criminal investigation.

Special attention is focused on computer trespassers. Under section 217 of the Act, an investigator may, without a warrant but with the permission of a computer's owner (such as a business whose computer system has been hacked), intercept communications of a computer trespasser that are being transmitted through the hacked computer. The investigator must have reasonable grounds to believe that the content of the communications will be relevant to an investigation; communications other than those to or from the trespasser may not be intercepted. Section 217 terminates on December 31, 2005.

Telecommunications services are less affected by section 222, which states that the Act does not "impose any additional technical obligation or requirement on a provider of a wire or electronic communication service or other person to furnish facilities or technical assistance." This section does, however, guarantee such providers reasonable compensation for any expenses incurred in providing assistance to authorities. Blanket immunity is granted to any provider of a wire or electronic communication service, landlord, custodian or other person who complies with a court order under the Foreign Intelligence Surveillance Act of 1978.

Upon request of a government agency investigating international terrorism, consumer reporting agencies are required confidentially to "furnish a consumer report of a consumer and all other information in a consumer's file to [an appropriate] government agency." The agency only needs to accompany the request with a certification that the information is necessary to "the agency's conduct or [international terrorism] investigation, activity or analysis."

If you have any questions, please contact John J. Kenney (j_kenney@stblaw.com), Joseph M. McLaughlin, (j_mclaughlin@stblaw.com) or Valerie Caproni (v_caproni@stblaw.com) at the firm's New York office (212 455-2000).

SIMPSON THACHER & BARTLETT LLP