ANTI-MONEY LAUNDERING & ECONOMIC SANCTIONS

RECENT DEVELOPMENTS: IMPLICATIONS FOR THE U.S. INSURANCE INDUSTRY

August 11, 2006

M. Beth Peters, Esq.
Aleksandar Dukić, Esq
Hogan & Hartson LLP [*]
Washington, DC

I. INTRODUCTION

U.S. economic sanctions programs impose a much wider range of prohibitions than a simple ban on exports of goods to far away rogue nations. These restrictions apply to the provision of services (such as insurance or reinsurance) and target individuals or entities who are outside the sanctioned country—in fact, they even target some persons and entities within the United States. Accordingly, even insurance companies that only operate domestically need to be aware of the broad restrictions under U.S. economic sanctions laws and regulations.

In addition, U.S. laws designed to prevent or detect laundering of money go well beyond concerns that a bag of "dirty" money may be used to buy goods or services—they address various stages of money laundering and impose numerous compliance and reporting obligations that are not limited to banks and other traditional financial institutions. Insurance companies need to understand and comply with U.S. anti-money laundering restrictions designed to prevent laundering of illicit funds. This paper analyzes U.S. economic sanctions and anti-money laundering provisions including compliance and reporting obligations that apply to insurance companies.

II. ECONOMIC SANCTIONS

A. Background

Governments around the world, as well as the United Nations, have imposed multilateral economic sanctions and trade embargoes against countries, entities, and individuals as a means to advance foreign policy and national security interests. However, the U.S. Government also imposes unilateral economic sanctions and trade embargoes which have the purpose of preventing the targeted countries, entities and individuals from benefiting from U.S. capital, goods, technology or services. This creates situations where U.S. persons must comply with restrictions not imposed on our trading partners or competitors overseas.

---

[*] M. Beth Peters is a partner and Aleksandar Dukić is an associate with the law firm of Hogan & Hartson LLP. The authors would like to thank Darshak Dholakia, a Summer Associate at Hogan & Hartson LLP, for his assistance.

B. U.S. Economic Sanctions Programs

The United States maintains comprehensive economic sanctions programs as well as more limited sanctions regimes. The U.S. Treasury Department's Office of Foreign Assets Control ("OFAC") administers and enforces both types of sanctions programs. 1/ The sanctions laws and regulations proscribe certain transactions with specific countries, entities and individuals. 2/ Penalties for violating economic sanctions laws may be civil or criminal, including monetary fines and imprisonment, and may be imposed on individuals, as well as organizations. 3/ Violations also can result in adverse publicity and reputational harm, even if the party involved were to negotiate a settlement with OFAC.

1. Sanctioned Countries

The U.S. Government has expanded economic sanctions against three countries: ***Burma***, ***North Korea*** and ***Syria***. In addition, the U.S. Government instituted new programs in February 2006 and June 2006 that target certain persons in ***Côte D'Ivoire*** and ***Belarus***, respectively. These sanctions are not territorial in nature (i.e., they do not apply to the Côte D'Ivoire, Belarus or their governments as a whole), as they only target designated persons and entities in their individual capacity. In addition, OFAC determined in April 2006 that Hamas, an organization already targeted by U.S. sanctions, has a property interest in transactions of the ***Palestinian Authority***. As a result of such determination, U.S. persons generally are prohibited from dealings with the Palestinian Authority but OFAC has issued six general licenses authorizing a number of transactions (these sanctions also are not territorial in nature). 4/ The U.S. Government has lifted economic sanctions completely against two countries: ***Libya*** and ***Sierra Leone***. 5/ In addition, sanctions against ***Iraq*** were substantially eased in 2004. 6/

2. OFAC Developments

OFAC is now using a new "institutional" approach to enforcement of economic sanctions, in contrast to previous transaction-specific enforcement policy. 7/ Voluntary disclosure of

---

1/ More information about OFAC and U.S. sanctions programs is available at http://www.treas.gov/offices/enforcement/ofac/index.shtml.

2/ OFAC regulations governing U.S. economic sanctions programs are found at 31 C.F.R. Parts 500-598.

3/ For most sanctions programs, civil penalties now include a fine of up to $50,000 per violation.

4/ For example, general licenses authorize payment of taxes and incidental fees to the Palestinian Authority, transactions with entities under the control of the Palestinian President, in-kind donations of medicine, medical devices and medical services, transactions ordinarily incident to travel to or from or employment, residence or personal maintenance within, the jurisdiction of the Palestinian Authority.

5/ U.S. sanctions against Libya were lifted on September 21, 2004, and all property previously blocked pursuant to the sanctions has been unblocked. As of July 13, 2006, Libya has been removed from the list of terrorist supporting countries so it is no longer subject to tighter export controls. Sanctions against Sierra Leone were lifted in January 2004.

6/ Iraq was removed from the State Department's list of terrorist-sponsoring countries, national emergency with respect to Iraq was revoked, and the licensing authority for exports and reexports of goods, software, and technology was transferred to the Commerce Department. It is still prohibited to deal with designated members of the former regime (SDNs) or trade in Iraq's cultural property and any other property blocked prior to May 23, 2003.

7/ OFAC has provided information about the elements of an effective OFAC compliance program in the *BSA/AML Examinations Manual* (June 2005; revised July 2006).

sanctions violations generally leads to at least a 50% mitigation of the penalty (OFAC will weigh mitigating and aggravating factors, if any, in proposing the penalty amount). With respect to penalties, the USA PATRIOT Improvement and Reauthorization Act of 2005, which was signed into law on March 9, 2006, increased the penalties for violations of the sanctions programs that are based on the International Emergency Economic Powers Act (e.g., Burma, Iran, Sudan, and Syria, among others). The maximum civil penalty amount was increased from $11,000 to $50,000 per violation, while the criminal penalty for willful violations by individuals was increased from 10 to 20 years imprisonment.

OFAC is using a new format for public disclosure of penalties and settlements resulting from these violations; there is a greater level of detail regarding the alleged violation, and information is disseminated in paragraph rather than table format. 8/ In addition, OFAC is contemplating industry-specific Enforcement Guidelines in the future. 9/

3. Specially Designated Nationals (SDNs)

The U.S. sanctions programs also prohibit transactions with persons and entities designated as terrorists, sponsors of terrorist activity and terrorist organizations, narcotics traffickers and kingpins, agents of sanctioned country governments, and proliferators of weapons of mass destruction. These persons and entities are designated by the U.S. Government as Specially Designated Nationals or Blocked Persons ("SDNs") and are included on the SDN list, which is maintained by OFAC. 10/ The SDN list currently contains more than 6,000 entries, including the names of individuals and entities, as well as other known information (e.g., aliases, date of birth, last known residential or business address, passport number etc.). The vast majority of SDNs are located outside of the United States; however, some are based in the United States, 11/ were born in the United States, 12/ or have U.S. Social Security numbers. 13/ OFAC regularly updates the SDN list due to frequent additions of newly designated persons and entities (occasionally, certain entries are removed from the SDN list).

Moreover, all citizens of Cuba (except those who are in the United States) and all entities owned or controlled by the Cuban Government or citizens of Cuba are considered SDNs, even though they are not specifically named on the SDN list. As a result, insurance companies should consider appropriate compliance activities to address this risk exposure (see Sections II.B.5 & 6 below for more details regarding sanctions compliance and screening activities).

8/ For more information, FAQs specific to the insurance industry are available on the OFAC website.

9/ On Jan. 12, 2006, OFAC published its new Enforcement Procedures for Banking Institutions and invited comments from the insurance industry and others (comments were due by Mar. 13, 2006).

10/ The SDN list is available at http://www.treas.gov/offices/enforcement/ofac/sdn/t11sdn.pdf.

11/ For example, Richard A. Chichakli in Texas, AERO Continente Inc. in Florida, Al-Haramain (U.S. branch) in Oregon, Ash Trading Inc. in Florida, Holy Land Foundation in Texas, IAC International Inc. in Florida, and Sepulveda-Iragorri Inc. in Florida.

12/ For example, Abdul Rahman Taha.

13/ For example, Julio C. Flores Monroy, Gregorio Gonzales Lopez, Raed M. Hijazi, and Abu Ahmad.

4. Scope of Restrictions

Under the comprehensive U.S. sanctions programs, a "U.S. person" generally may not, without a license or authorization from the U.S. Government, 14/ engage in any of the following:

- Export or import, directly or indirectly, goods, services or technology to and from, a sanctioned country;
- Enter into a contract involving, or otherwise provide services to, a sanctioned country, including an entity or individual located in a sanctioned country;
- Engage in any transaction with persons and entities designated as SDNs;
- Approve or facilitate any of the above activities; and
- Evade provisions of the sanctions regulations.

U.S. persons also must "block" (freeze) property and property interests of SDNs, and certain sanctioned country governments, that are within the possession or control of a U.S. person. 15/ This includes funds received from or held on behalf of, or a policy involving, an SDN. For example, a U.S. insurer who receives a premium payment from an SDN must place such funds into a blocked, interest-bearing account at a U.S. financial institution. In addition, the receipt of such blocked property must be reported to OFAC, as set forth in Section II.C below. Similarly, if a U.S. insurer has an existing policy issued to a person who subsequently becomes an SDN, the insurance company must "block" such policy on its books, preventing any further activity or performance under the policy, and must file a blocked property report with OFAC.

The prohibitions on exportation and importation of services generally are very broad and apply to services provided or received, directly or indirectly, to or from a sanctioned country or an SDN (e.g., issuing a policy to a company in the United States that also extends coverage to a foreign incorporated subsidiary's activities in Iran generally is considered a prohibited exportation of a service to Iran). In addition, the comprehensive U.S. sanctions programs have broad prohibitions on approval and facilitation by U.S. persons. 16/ For example, U.S. persons are prohibited from participating in, approving or facilitating, aiding or otherwise supporting activities by foreign persons involving a sanctioned country where such actions would constitute violations of the sanctions if engaged in by a U.S. person. Similarly, OFAC interprets the facilitation provision to prohibit a U.S. person from altering its operating policies or procedures, or those of a foreign affiliate, in order to permit a foreign affiliate to engage in transactions involving a sanctioned country that previously required the approval or participation of the U.S. person. Moreover, OFAC regulations prohibit U.S. persons from engaging in any transaction

---

14/ There are comprehensive OFAC sanctions against Cuba, Iran, and Sudan; while the OFAC sanctions against Syria currently are narrow, the U.S. export controls are extremely broad. For most sanctions programs, authorization to conduct a transaction is obtained from OFAC; for certain transactions, U.S. persons must file requests for authorization with the Commerce Department's Bureau of Industry and Security (BIS).

15/ Not all of the country-specific sanctions programs have "blocking" provisions (for example, the current U.S. sanctions against Iran do not block the property of the Government of Iran). The broadest restrictions are in the Cuba sanctions program. The terms property and property interests are defined broadly to include all forms of financial interests, whether tangible or intangible, such as insurance policies, claims, bank deposits, savings accounts, real property, leases, letters of credit, money, securities, as well as contracts of any nature. *See generally* 31 C.F.R. §§ 515.311, 538.310.

16/ *See generally* §§ 538.206, 538.407, 560.208, 560.417.

that evades or avoids, or has the purpose of evading or avoiding, the restrictions imposed by U.S. sanctions programs.

All of the U.S. sanctions programs apply to "U.S. persons," which is defined broadly to include:

- Entities organized under U.S. law, and their employees (e.g., U.S. corporations, U.S. institutions and organizations);
- All U.S. citizens and U.S. lawful permanent residents (also known as "green card" holders) wherever they are located;
- All people and organizations physically present in the United States, regardless of citizenship; and
- All foreign branches of U.S. businesses and other U.S. organizations.

For purposes of U.S. sanctions against Cuba and North Korea, however, the sanctions apply more broadly to "persons subject to U.S. jurisdiction," which is defined to include foreign-incorporated subsidiaries of U.S. companies as well. 17/

5. Compliance Issues for Insurers

For the insurance industry, economic sanctions generally mean that prohibited transactions may include:

- issuing a policy;
- underwriting insurance and reinsurance contracts;
- accepting premiums;
- paying claims;
- furnishing services;
- terminating or commuting a policy; or
- assisting or facilitating the above activities.

With respect to policy issuance, there are three possible scenarios involving OFAC sanctions issues:

(a) Issuing a policy to an SDN (i.e., the policy is unlawful upon issuance)—Policy issuance was a violation and the insurer is required to block the policy (and any premium money received) and file a blocked property report. Also, the insurer cannot pay any claims, cannot cancel, commute or otherwise deal in this policy without a license from OFAC.

(b) Policy was lawful when issued but the insured subsequently becomes an SDN through designation by the U.S. Government or through change of ownership, control or management (such that the insured becomes an SDN)—Policy issuance was not a violation but the insurer is required to block the policy (and any premium payment received after the insured became an SDN) and file a

17/ *See id.* §§ 500.329, 500.330. This definition also includes any entity owned or controlled by "U.S. persons."

blocked property report. Also, the insurer cannot pay any claims, cancel, commute or otherwise deal in this policy without a license from OFAC.

(c) No SDN is involved (either at policy issuance or subsequently) but the policy provides coverage for risks in or involving a sanctioned country (e.g., a policy issued to a U.S. company provides health coverage for workers who engage in unlicensed activities in Sudan)—Policy issuance (the provision of coverage) is a violation but there is no blocking or reporting required. No claim payments involving in any way a sanctioned country are allowed without an OFAC license (e.g., a loss arose in a sanctioned country or a third-party claimant is from a sanctioned country). Other claim payments under the policy would not necessarily present an OFAC compliance issue but they should be carefully reviewed. The insurer is not prohibited from canceling, commuting, or otherwise dealing in this policy.

In addition, insurers need to be aware that economic sanctions issues could arise when:

- the insurer undergoes a corporate restructuring (e.g., moving activities from offshore to the United States or combining operations of U.S. and overseas business units)
- the insurer offers internet-based services or account access
- personnel matters are involved (e.g., hiring and screening of foreign nationals)
- the insurer relocates U.S. personnel overseas (e.g., executives transferred abroad to oversee or run operations of foreign subsidiaries)
- U.S. persons serve as Board members of the insurer's non-U.S. subsidiaries
- Delegated Underwriting Authority ("DUA") or Third Party Administrator ("TPA") arrangements are present

(i) *Life and Health Insurance*

Insurers providing life and health coverage must be careful, especially when group policies are involved, in order to prevent claim payments to SDNs. If the named insured on a group policy is not an SDN but the insured's employee who files a claim under the policy is an SDN, the insurer may rely on OFAC's analysis of worker's compensation policies to argue that the group policy itself is not blocked even if a particular claimant is an SDN (that claimant's interest in the policy would be "blocked" and no claim payment would be permitted without an OFAC license but the entire group policy, arguably, would not have to be considered blocked).

Claims from overseas (or from third-party claimants) generally involve a higher risk for sanctions compliance and should be closely scrutinized. Also, insurers may want to inquire whether a specific license issued by OFAC exists for the underlying activity. For example, in reviewing a worker's compensation claim for a loss in a sanctioned country submitted under a Defense Base Act (DBA) policy issued to a U.S. Government contractor, the insurer may want to ask whether the contractor was covered by an OFAC license (e.g., OFAC has issued a license to the U.S. State Department for activities of its contractors who are building the U.S. Embassy in Burma; OFAC also issued a license to the U.S. Agency for International Development for activities of its contractors working on humanitarian projects in Sudan).

With respect to "conditional coverage," where an agent accepts an insurance application and premium payment and the coverage starts immediately (prior to underwriting), insurers may want to use specific policy language in the contract and/or application forms to add a condition related to economic sanctions. By adding such condition, the insurer can prevent inadvertent provision of coverage to an SDN prior to receiving the application from the agent and conducting its own screening (essentially, the new language would exclude conditional coverage in cases where the applicant is an SDN).

With respect to blocked policies, insurers are permitted to record on their books increases and decreases in cash value (e.g., on a whole life or universal life policy), deduct "cost of insurance" and perform similar administrative account maintenance on blocked policies, without a specific license from OFAC.

Life insurers should note that a change of beneficiaries on an existing policy, where a new beneficiary is an SDN, could trigger the blocking requirement. Therefore, insurers should review all actions taken on a policy during the validity period.

Insurers providing travel-related products (e.g., travel and accident policies), should note that most sanctions programs do not restrict the ability of U.S. persons to travel to a sanctioned country, with the exception of the U.S. sanctions against Cuba. Travel to Cuba must be authorized by OFAC. Accordingly, insurers should ensure that their coverage extends only to travel to Cuba that is authorized by OFAC (coverage provided to an unlicensed traveler could result in a prohibited exportation of an insurance service to Cuba).

(ii) Property and Casualty Insurance

Property and casualty ("P&C") insurers generally should be wary of risks that would be covered by the policy but are not apparent from the insured's location or principal base of business. 18/ U.S. insurers may not want to offer worldwide P&C coverage without using restrictive endorsements to exclude coverage related to sanctioned countries. Also, the companies may want to train P&C underwriters to spot sanctions exposure by reviewing all materials in the underwriting file and assessing all properties or persons covered by the policy (not just the named insured or the principal location). In addition, insurers using screening software may want to screen a number of relevant policy fields, not simply the insured's name and principal place of business (e.g., have the software screen all locations for properties or entities listed on the policy).

Marine insurance products (e.g., open cargo, hull) present additional risks. For example, reporting on a "declaration" basis on an open cargo policy would mean that the insurer would learn about the destination only after the fact (post-shipment) and yet the insurance coverage could have been extended for a shipment to a sanctioned country (absent exclusionary policy language). Also, risks are present if the insured is provided with blank insurance certificates that

18/ For example, a French company may have a property located in Sudan listed among all other properties on an addendum or endorsement to the policy, or a Brazilian company seeking a CGL policy with worldwide coverage receives 5 percent of its annual revenue from activities in Cuba.

would accompany individual shipments, or if the insured is allowed to complete and print certificates online, without having a block for sanctioned country destinations. When U.S.-origin goods are involved in a particular marine shipment, U.S. export control issues are involved and the insurer should avoid the provision of insurance coverage for shipments that are made in violation of U.S. export control laws. With respect to hull coverage, insurers should recognize that a number of vessels are designated as SDNs. Moreover, due to recent changes in the North Korea sanctions, U.S. persons cannot extend insurance coverage for any North-Korean flagged vessels.

Case Study:

Q. An open cargo policy is issued to a Canadian freight forwarder (FF) who reports shipments on declaration basis. The policy offers worldwide cover for all shipments handled by the policyholder. XYZ Co., a customer of FF, makes three shipments from Canada to Sudan, one of which results in a claim (the claimant is a school in Sudan). The U.S. insurer becomes aware of all the shipments and the claim well after the shipments were made. What do we do now?

A. The provision of insurance for all 3 shipments would be viewed by OFAC as a prohibited exportation of services to Sudan. The insurer cannot make the claim payment to an entity in Sudan without a license from OFAC (a license may not be granted). If license is pursued, the insurer may need to disclose the insurance coverage provided for the other 2 shipments to Sudan, without authorization (in order to get the benefit of voluntary disclosure mitigation, the license application would have to be accompanied by a separate disclosure).

6. Compliance and Screening

OFAC regulations do not mandate that U.S. companies use screening software to check persons or entities against the SDN list in order to ensure compliance with U.S. sanctions programs. Because the applicable regulations prohibit any dealings by U.S. persons with individuals or entities on the SDN list, the use of screening software is advisable, especially when there is a large number of persons or transactions that need to be screened. Of course, an insurer with only domestic exposure and a limited amount of policies could achieve compliance by manually comparing the names to the entries on the SDN list, which is available online as described above. However, this approach may not be feasible if the insurer is trying to screen a large number of policies or transactions (e.g., a large insurance company with a significant number of premium and claim payments processed daily).

As part of the compliance plan, insurance companies should:

- Determine whether a person or entity from a sanctioned country is involved in any way in the contemplated policy or transaction (e.g., as a named insured, a third-party claimant, etc.); and
- Check the names of the persons involved against the SDN list (either manually, using the list published on OFAC's website, or through the use of a screening software).

Because the SDN list changes frequently, as newly designated persons or entities are added, regular vigilance is necessary. To ensure compliance, screening should be done on a regular basis. If the insurer were to conduct screening only at the outset of a relationship (e.g., policy issuance, entry into a vendor contract), it would confirm that the company can engage in the contemplated transaction (e.g., issue a policy or enter into a vendor contract) but that approach would not capture any subsequent changes that may affect the relationship. Without periodic screening, there would be some exposure for the insurer because it would be unaware if insureds, beneficiaries, third-party claimants, vendors or other contract parties subsequently became designated as SDNs or if they were subject to new sanctions programs. As such, the insurer would not be able to comply timely with the blocking and reporting obligations and could inadvertently be conducting transactions that it is no longer authorized to perform (e.g., while it is permitted to issue a policy to an insured before his/her SDN designation, no payments could be made to him/her after the designation, absent a specific license from OFAC). In light of the volume of policies and transactions as well as the frequency of changes on the SDN list, the most effective way to ensure compliance is through periodic, automated screening. The interval in which an insurer conducts "batch" screening is based on the entity's assessment of its OFAC-related risks.

Recommended best practices to ensure compliance include:

- Perform a risk-assessment and implement compliance procedures based on such assessment
- Use screening software for automated, periodic screening
- Use exclusionary policy language to prevent coverage that is not permitted under OFAC regulations (OFAC highly recommends the use of restrictive policy language, which can minimize or eliminate exposure and also serves as a mitigating factor in case of a violation)
- Periodically train employees with respect to sanctions compliance
- Establish and maintain good recordkeeping and auditing functions
- Remain current and keep abreast of changes in economic sanctions laws

C. Reporting Requirements

Under OFAC regulations, U.S. persons are required to file a blocked property report with OFAC within 10 days of receiving funds from an SDN (or within 10 days from the date a person or entity is designated as SDN if, at the time of the designation, the U.S. person has an existing contract with, or holds funds in an account on behalf of, the person or entity designated as SDN). In addition, blocked property reports must be filed if the U.S. person receives funds from, or holds funds on behalf of, a sanctioned country government (or any of its agencies, instrumentalities, or entities owned or controlled by it) that is subject to the blocking provisions, such as Cuba and Sudan. After filing the initial blocked property report, a U.S. person must also file an annual report, listing all blocked property received over the course of the year. Annual reports are due on Sept. 30, listing all blocked property (policies, funds) held as of June 30.

Policies can be blocked on the insurer's books, and related funds may be kept in an "omnibus" account as long as the insurer can credit interest and attribute principal to each blocked party.

Case Study:

Q. An existing policyholder is designated as an SDN on Jan. 15. He pays his semi-annual premium on Mar. 15. In August, during the renewal process, the insurer realizes that he is an SDN. Can the insurer return the premium and terminate the policy immediately?

A. No. The premium payment should have been placed in a blocked, interest-bearing account (could be an omnibus account). The policy should have been blocked and reports should have been to OFAC by Jan. 25 (to report the blocked policy) and by Mar. 25 (to report the blocked payment). Even though late, the insurer should still block everything now and report to OFAC. With respect to policy termination, the company cannot terminate the policy without a specific OFAC license but the insurer can let the policy lapse (i.e., wait for the policy term to expire, if there is no automatic renewal provision in the policy).

III. ANTI-MONEY LAUNDERING/USA PATRIOT ACT

A. Background

The United States imposes anti-money laundering ("AML") restrictions to protect the integrity of the U.S. financial sector and to prevent criminals and terrorists from abusing the U.S. financial system for their illicit activities. Money laundering involves disguising financial assets so they can be used without detection of the illegal activity that produced them. Through money laundering, the criminal transforms the monetary proceeds derived from criminal activity into funds with an apparently legal source. There are three stages to money laundering:

1. *Placement* – illegally derived funds are placed into the stream of commerce;
2. *Layering* – one or more transactions to disguise the true source of the funds; and
3. *Integration* – money is repatriated into the economy in its disguised form, with the appearance of being "clean" and coming from a legitimate source. 19/

Most people think of the placement stage as "the" money laundering. However, the other two stages also are an integral part of the process and those two stages may involve transactions with businesses, such as insurance companies, that are not typically viewed as "gatekeepers" for AML purposes. In order to track the flow of funds, the U.S. Government has established a fairly

19/ For example, a person purchases a $5 million whole life policy purchased with "dirty" money (*Placement*), through a series of small cash payments in an attempt to avoid triggering the reporting threshold (the practice known as "structuring" or "smurfing"). The policy's cash value is then built up by funds that passed through a number of banks/jurisdictions (*Layering*). Finally, the launderer may take out a maximum loan under the policy, therefore receiving "clean" money from the insurer (*Integration*).

complex reporting system, through the Bank Secrecy Act ("BSA"), 20/ as amended by the Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism Act of 2001 ("USA PATRIOT Act"), 21/ Treasury regulations, and the Internal Revenue Code ("IRC"). As explained below, certain reporting obligations apply to all businesses in the United States. The BSA contains additional AML provisions that apply to a wide range of "financial institutions," which are very broadly defined to include businesses beyond those traditionally viewed as within the financial industry.

Because terrorists engage in money laundering to fund their illicit activities, U.S. AML laws and regulations are designed to disrupt and prevent terrorism-related money laundering activities. Furthermore, the same laws strive to disrupt and prevent terrorist financing, which represents the opposite of money laundering (i.e., legally derived funds are used for illicit activities, to fund terrorist acts or organizations).

U.S. laws designed to prevent and detect money laundering and terrorist financing are administered by the Treasury Department's Financial Crimes Enforcement Network ("FinCEN"). 22/ *U.S. Money Laundering Threat Assessment*, published by various U.S. Government agencies in December 2005, identifies AML risks presented by certain insurance policies (life and annuity). 23/

B. AML Provisions in the Bank Secrecy Act/USA PATRIOT Act

As described in more detail below, certain AML provisions apply to all businesses in the United States, such as the obligation to report the receipt of cash in excess of a certain amount or the receipt of cash that was physically transported across U.S. borders (also in excess of a certain amount). These provisions predate the enactment of the USA PATRIOT Act and all insurance companies should be aware of, and must comply with, these reporting obligations. The majority of AML provisions addressed in this section, however, apply only to covered "financial institutions," as that term is broadly defined under the BSA.

1. The Definition of "Financial Institution"—Are All Insurance Companies Covered?

The term "financial institution" is broadly defined in the BSA to include businesses beyond those traditionally viewed as financial institutions such as banks and credit unions—specifically, the definition also includes mutual funds, brokers/dealers in securities, insurance companies, "loan or finance companies," casinos, pawnbrokers, dealers in jewels and precious

---

20/ 31 U.S.C. § 5311 *et seq.*

21/ Pub. L. 107-56 (Oct. 26, 2001). Title III of the USA PATRIOT Act, which is titled the International Money Laundering Abatement and Financial Anti-Terrorism Act of 2001, provides the Secretary of the Treasury and other departments and agencies of the federal government with enhanced authority to identify, deter, and punish international money laundering.

22/ More information about FinCEN is available at: http://www.fincen.gov/index.html.

23/ The complete *Money Laundering Threat Assessment* can be found on the following Department of the Treasury Web site: http://www.treas.gov/press/releases/reports/js3077_01112005_MLTA.pdf.

metals, car dealers, and persons engaged in real estate settlements and closings, etc. 24/ None of these terms are defined in the BSA and the Treasury Department is taking a risk-based, industry-specific approach in issuing regulations to implement various BSA/USA PATRIOT Act provisions and to define the types of businesses covered by these AML requirements.

FinCEN's regulations implementing AML compliance program and suspicious activity reporting requirements have defined the term "insurance company" to include only those insurance companies that are issuing or underwriting a "covered product." Under FinCEN's regulations, the term "covered product" means:

(1) a permanent life insurance policy, other than a group life policy;

(2) an annuity contract, other than a group annuity contract; and

(3) any other insurance product with features of cash value or investment.

These AML requirements are applicable only to "covered products," not to other insurance products that the company may be offering as well. In addition, FinCEN indicated that if an insurance company were to cease to issue or underwrite "covered products," it would no longer be subject to the AML compliance program and suspicious activity reporting requirements. Moreover, FinCEN confirmed that none of the following products are considered "covered products:" group insurance products; term life (including credit life) products; property, casualty, health and title insurance products; charitable annuities; contracts of indemnity and structured settlements (including worker's compensation payments); and reinsurance and retrocession contracts.

However, certain "information sharing" requirements under sec. 314, as explained below, are applicable to all insurance companies. In addition, to the extent that insurance companies have subsidiaries that are registered brokers/dealers in securities (i.e., those offering insurance products that are covered by the definition of "securities"), are registered or chartered as banks, or are organized as mutual funds, those subsidiaries also are covered "financial institutions" and must comply with the applicable BSA requirements for brokers/dealers, banks, or mutual funds, respectively. The entire insurance company would not become subject to the BSA simply by having a subsidiary that is a registered broker/dealer; instead, the subsidiary itself must comply with various AML provisions and the insurance company generally might be exempt, unless it engages in activities involving "covered products" noted above.

Based on the foregoing, insurance companies that do not offer (or have no subsidiaries that offer) "covered products," products covered by the definition of "securities" under U.S. securities laws, and that are not registered as a bank or a mutual fund, currently are not subject to specific AML provisions in the BSA that apply to "financial institutions," with the exception to "information-sharing" requirements that apply to all insurance companies. In addition to information sharing, those insurance companies are subject to reporting requirements that apply to all U.S. businesses and institutions, as set forth in Sections III.C.2 and C.3 below.

24/ *See* 31 U.S.C.A. § 5312(a)(2).

2. Key AML Provisions That Apply to "Financial Institutions"

Key AML provisions in the BSA, as amended by the USA PATRIOT Act, that currently apply (or will apply upon issuance of the implementing regulations) to "financial institutions" such as insurance companies are:

- **Sec. 352** – AML Compliance Program Requirements
- **Sec. 326** – Customer Identification and Verification Requirements (also known as "Know Your Customer" or "KYC" requirements)
- **Sec. 314(a)** – Information Sharing and Cooperation with Law Enforcement
- **Sec. 311** – Designation of "Primary Money Laundering Concerns" and Imposition of "Special Measures" against such designated entities or jurisdictions.
- **Suspicious Activity Reporting ("SAR")** (also called Suspicious Transaction Reporting) – see Section III.C for more details

3. Section 352 – AML Compliance Programs

Final rule implementing sec. 352 AML Compliance Program requirements for insurance companies became effective May 2, 2006. As of that date, insurance companies that issue or underwrite "covered products" are required to establish and implement an AML Compliance Program, based on a "risk assessment" of its products and services. Accordingly, lower risk products/services or transactions may warrant fewer procedural controls; risks can be jurisdictional, product-related, service-related or customer-related. As explained above, this requirement applies only to U.S. insurance companies that issue or underwrite permanent life policies (other than group life), annuity contracts (other than group annuities), or other insurance products with cash value or investment features. 25/ While FinCEN does not expect insurance companies to prevent all money laundering, it does expect them to take prudent steps to comply.

Each AML program must contain the following: (1) designation of a compliance officer (with sufficient authority to carry out AML responsibilities); (2) establishment of internal policies, procedures, and controls related to "covered products"; (3) provision for employee training (may be in-house training); and (4) an independent audit function (the insurer should not use its compliance officer as an "independent" auditor). The AML Compliance Program should be approved by senior management. Insurers may delegate a part of the required AML functions to agents but the insurer would retain liability for the agent's actions, with limited exceptions. Agents or brokers are not required to have their own programs, but instead should be integrated within the insurer's AML program and their compliance should be monitored.

Policies that support the insurer's AML efforts include:

- Conducting risk assessment of the institution's activities and services

25/ Sec. 352 does not apply to group insurance products, charitable annuities, reinsurance and retrocession products, contracts of indemnity and structured settlements, and term (incl. credit) life, property, casualty, health, or title insurance. All insurance companies not covered by section 352 must still comply with the existing cash reporting requirements (FinCEN 8300 and FinCEN 105 reporting).

- Identifying high risk transactions and communicating "red flags" to relevant employees
- Monitoring account transactions, including attempted "structuring" or "smurfing" (employees should not focus exclusively on the "placement" stage and should be mindful of possible abuse through "layering" and "integration")
- Requiring reporting of suspicious transactions and cash transactions (as set forth in Section III.C below, the institution has to determine whether reporting of a cash transaction is required (by filing the 8300 form) or whether a Suspicious Activity Report (SAR) is required or warranted in a particular case)
- Establishing "Know Your Customer" procedures, which may be integrated within the AML Compliance Program

4. Section 326 – Customer ID/Verification ("Know Your Customer")

Section 326 requirements are not yet applicable to insurance companies. FinCEN has yet to issued proposed regulations for insurers, which are expected to apply to the same insurance companies that are also subject to sec. 352 AML compliance program requirements (please note that the sec. 326 final rule for registered broker/dealers and mutual funds is already in effect). Once implemented through FinCEN's final rule, sec. 326 will require insurance companies to establish and implement a Customer Identification Program ("CIP"), which likely will be risk-based and appropriate for the size and type of activity involved. The purpose of a CIP will be to identify the institution's new customers and to verify their identity. Although "Know Your Customer" regulations for insurance companies have yet to be proposed, they will likely be similar to the final rules for registered brokers/dealers and mutual funds. Under those requirements, institutions are required to:

- Verify the identity of any person seeking to open a new "account," using reasonable procedures for identifying persons and entities
- Develop procedures responding to circumstances where a reasonable belief about the true identity cannot be formed
- Maintain records of identifying information
- Determine whether the person appears on any lists of known or suspected terrorist or terrorist organization provided by any government agency (at present, OFAC's SDN list is the only such list that insurers would need to check)

5. Section 314(a) – Information Sharing/Cooperation with Law Enforcement

Final rule implementing section 314(a) information sharing requirements on covered financial institutions became effective in September 2002. A law enforcement agency that wants to search the records of a particular financial institution to see whether a person or entity that is the target of an investigation is maintaining account(s) or other relationship(s) with U.S. financial institutions can submit a request to FinCEN. Upon reviewing the request, FinCEN would make a determination whether the request qualifies for section 314(a) purposes and, if so, FinCEN would send the request to one or more financial institutions. The request from FinCEN may ask the institution to search its records for any information on a particular person or entity identified in the request.

There is no formal exemption for insurance companies from section 314(a) information requests ("314(a) requests"). FinCEN previously informally advised the authors that 314(a) requests were being sent only to financial institutions that are required to have an AML program, such as banks, credit unions etc. However, some insurance companies received 314(a) requests since that time, even before the AML program requirements for insurers had been finalized. Accordingly, any insurance company should be prepared to receive a 314(a) request, which may ask the company to search its records for any information on a particular person or entity. Insurance companies should designate one or more persons as those responsible to take action on a 314(a) request.

6. Section 311 – "Primary Money Laundering Concerns"

Section 311 authorizes the U.S. Government to designate entities or jurisdictions as "primary money laundering concerns" ("PMLC") and to impose one or more of the "special measures" authorized by the statute. The most comprehensive special measure requires covered U.S. financial institutions to terminate all correspondent account relationships with PMLCs, and prevents existing correspondent accounts held on behalf of third parties to be used indirectly for or on the benefit of PMLCs. Because insurance companies generally do not have correspondent account relationships with foreign entities, the PMLC determinations by the U.S. Government and related imposition of special measures should not directly affect insurers in most cases. That said, involvement of a PMLC in a contemplated insurance transaction could be a "red flag" that warrants closer scrutiny of the account for money laundering risks.

To date, the U.S. Government has taken the following actions pursuant to authority set forth in section 311 (there have not been any insurance-related designations yet): 26/

- **Nauru**—designated as PMLC and "special measures" were proposed (termination of correspondent accounts involving Nauru financial institutions)
- **Burma and 2 Burmese banks**—designated as PMLCs and "special measures" were imposed (termination of correspondent accounts)
- **Commercial Bank of Syria (CBS)**—CBS and its subsidiary were designated as PMLCs (Syria as a country, however, has not been designated as PMLC) and "special measures" were imposed (termination of correspondent accounts)

7. Financial Action Task Force (FATF)

On the international level, the Financial Action Task Force on Money Laundering ("FATF") is an inter-governmental body whose purpose is the development and promotion of policies, both at national and international levels, to combat money laundering and terrorist financing. 27/ FATF issues recommendations to its members and maintains a list of Non-Cooperative Countries and Territories ("NCCT") identified by FATF as having significant

26/ This summary does not include a complete list of entities that have been designated as PMCLs but have yet to be subject of a final rule imposing a particular special measure against them (for example, Infobank from Belarus, First Merchant Bank from the Turkish Republic of Northern Cyprus and its subsidiaries, etc.)

27/ More information regarding the FATF is available at: http://www1.oecd.org/fatf.

deficiencies in their AML systems, or not having any systems at all. At present, there is only entry on the NCCT list: Myanmar (Burma). 28/

Countries are added to or removed from the NCCT list based on their efforts in implementing legislation and adequate procedures to address money laundering and terrorist financing. Inclusion on this list can have a significant adverse effect on the ability of the country's government, businesses and citizens to conduct cross-border financial transactions, especially with or involving U.S. financial institutions.

C. Reporting Requirements

As noted above, the U.S. Government has established a fairly complex reporting system through the BSA and the USA PATRIOT Act. Reporting obligations related to cash transactions (receipt or transportation cross-border) apply to all persons in the United States (including all insurance companies). The obligations to file mandatory reports of suspicious activities applies only to certain financial institutions covered by the BSA for which FinCEN has issued final regulations that require such reporting (of course, financial institutions not covered by the mandatory suspicious activity reporting could file voluntary reports on suspicious activities). As a result, this overview addresses the following types of reporting obligations:

- Suspicious Activity Reporting (SAR)
- Reporting of cash transactions (CTR or FinCEN 8300 reports)
- Reporting of transportation of currency across border (FinCEN 105) 29/

1. Suspicious Activity Reporting (SAR)

Under the BSA implementing regulations, only insurance companies that are subject to sec. 352 AML compliance program requirements (i.e., those that issue or underwrite "covered products") are required to report suspicious transactions by filing Suspicious Activity Reports ("SARs") using form FinCEN 108 (SAR-IC). 30/ SAR filing remains voluntary for all other insurance companies, unless the insurance company is considered a registered broker/dealer, mutual fund or a bank (in which case, SAR reporting would be mandatory).

Elements of mandatory SAR reporting:

- $5,000 threshold to trigger mandatory reporting (if a transaction is below $5,000, voluntary SAR may be filed)
- Suspicious transactions are not limited to those involving cash or cash equivalents (SAR reporting applies to wire transfers, checks etc.)
- Insurance agents and brokers are not required to file SARs (the insurer is required to obtain all relevant information from its agents/brokers and file SARs, where appropriate)

28/ Nigeria was removed from the NCCT list in June 2006.
29/ FinCEN Form 105 was formerly Customs Form 4790.
30/ Until form FinCEN 108 (SAR-IC) is published and becomes effective, insurance companies should use form FinCEN 101 (SAR by the Securities/Futures Industries).

- If suspicious activity relates to the receipt of cash, the insurer may need to file both FinCEN 8300 (cash reporting) and FinCEN 108 (SAR-IC)
- File SARs within 30 days, in most cases
- Document retention period is 5 years
- After filing a SAR, the insurer is prohibited from disclosing the filing to the customer (i.e., there is no "tipping" of customers regarding SAR filing)
- The BSA provides a "safe harbor" – protects the insurer from liability for disclosures made in a SAR report

A particular transaction would be considered "suspicious" if the insurance company knows, suspects, or has reason to believe that the transaction:

- Involves funds derived from illegal activity or is intended to hide or disguise such funds
- Is designed, through structuring or otherwise, to evade cash reporting requirements
- Has no business or apparent lawful purpose or is not the sort of transaction in which the particular customer would be expected to engage (and the insurance company knows of no reasonable explanation for the transaction)
- Involves the use of the insurance company to facilitate criminal activity (e.g., the use of legally derived funds that are suspected of being used for a criminal purpose such as terrorist financing)

Determinations with respect to mandatory SAR filing are made based on all the facts and circumstances relating to the transaction. In order to be in a position to determine whether a particular activity is suspicious, the insurance company has to know the customer's usual activities. The institution's SAR monitoring may, and should, be integrated within the establishment and implementation of an AML Compliance Program under section 352. Insurance companies should not rely solely on their existing measures to combat fraud in lieu of having a formal Compliance Program – such measures may be useful for SAR purposes but not sufficient to satisfy the BSA requirements.

Insurance companies should generally watch for transactions that do not make economic sense or are unusual for the particular customer (or customer type). FinCEN provides some examples of these "red flags" for insurance companies, including:

- The purchase of an insurance product that appears inconsistent with a customer's needs
- Any unusual method of payment, particularly by cash or cash equivalents (if, in fact, unusual)
- The purchase with monetary instruments in structured amounts
- The early termination of an insurance product, especially at a cost to the customer, or where cash was tendered and/or refund check is directed to an apparently unrelated third party
- The transfer to the benefit of an apparently unrelated third party

- Little or no concern by a customer for the investment performance of a product, but much concern about early termination features
- The reluctance by a customer to provide identifying information when purchasing an insurance product, or the provision of minimal or seemingly fictitious information
- The borrowing of the maximum amount available soon after purchasing the product

Also, insurance companies should review more carefully:

- Customers from countries on the NCCT list (or sending payments from or requesting payments to such countries)
- Customers from narcotic source countries (e.g., Colombia—there is both AML risk and OFAC risk because a number of SDNs are located in Colombia);
- Transactions involving PMLCs
- Pattern of frequent claims
- Customers acting for others
- Pattern of "round trip" loan transactions (e.g., taking out a loan, followed by repayment and another loan within a short time frame)
- Viatical settlements

2. Reporting of "Cash" Transactions (CTR or FinCEN 8300 Reports)

All U.S. businesses and institutions have been subject to "cash" reporting requirements under section 6050I of the IRC and applicable Internal Revenue Service regulations, even before the enactment of the USA PATRIOT Act. 31/ The USA PATRIOT Act's section 365 and FinCEN's implementing regulations codified these reporting requirements within the BSA (FinCEN's regulations also clarified that only one report needs to be filed, separate reports under IRC and BSA are not required). 32/ Under the applicable regulations, any person who, in the course of a trade or business, receives "cash" in excess of $10,000 in one transaction (or two or more "related transactions") is required to report the receipt of cash by filing FinCEN Form 8300. Financial institutions covered by the BSA (such as insurance companies issuing or underwriting "covered products") are subject to the same reporting requirements, albeit under a different regulatory provision, and are required to report the receipt of cash by filing FinCEN Form 104, Currency Transaction Report ("CTR"). 33/

Accordingly, all insurance companies are required to report the receipt of "cash" that totals more than $10,000 in single transaction (or a series of related transactions). Premium payments in installments would be considered a "series of related transactions" so if payments are made in "cash," the insurer would need to assess whether the reporting requirement is triggered.

31/ *See* 26 C.F.R. § 1.6050I-1.
32/ *See* 31 C.F.R. § 103.30.
33/ *Id.* § 103.22.

For purposes of this reporting obligation, the term "cash" includes coin and currency as well as enumerated monetary instruments (i.e., a cashier's check, bank draft, traveler's check, and money order) having a face amount of $10,000 or less but only when such monetary instrument is received:

- In a "designated reporting transaction" (i.e., a retail sale of a consumer durable, a collectible, or a travel or entertainment activity), or
- In a any transaction in which the recipient knows that such monetary instrument is being used to avoid triggering the reporting requirement (i.e., the recipient knows that the instrument is being used to "structure" payments to avoid triggering the $10,000 threshold). 34/

Case Study:

Q. A foreign national purchases a $5 million whole life policy by paying the premium in advance, with $9,000 in cash and 3 money orders worth $4,000 each. He also tells the agent that it would be "so much easier" if he were "allowed" to pay the whole amount in cash, all at once. A week later, he pre-pays additional premium by a wire transfer of $45,000 from an off-shore trust account. He then takes out a loan in the amount of $50,000 and repays it within a month, with another funds transfer from a different off-shore account. He is now asking for a second loan of $50,000 and I'm starting to get suspicious. What should I do?

A. With respect to his initial premium payment, you may have to file a FinCEN 8300 for receipt of cash or "cash equivalents" in excess of $10,000 in a series of related transactions. Even though money orders had face value of less than $10,000, you may have reason to know that he's been "structuring" his money orders to avoid triggering the reporting threshold.

With respect to the policy loans (and in light of his initial premium payment), you also may have to file a mandatory SAR because the activities involve more than $5,000, are inconsistent with normal account activity, and are unusual in frequency and type.

You would have 30 days from his last loan request to file a SAR.

You cannot tell the insured that a SAR has been filed and you would have to keep all the records related to these transactions for 5 years from the date of SAR filing.

3. Reporting of Cross-Border Transportation of "Cash" (FinCEN 105)

Under applicable Treasury regulations, a person in the United States who receives currency or "monetary instruments" in an aggregate amount exceeding $10,000, which have been transported, mailed or shipped to the United States from a third country, must report the receipt of such cash or monetary instruments. 35/ The report is filed by submitting FinCEN

34/ *Id.* § 103.30(c)(1); 26 C.F.R. § 1.6050I-1(c)(1).
35/ *See* 31 C.F.R. § 103.23.

Form 105 (formerly Customs Form 4790). This reporting obligation does not apply if the person who transported or mailed the cash/monetary instruments that exceed the threshold amount had already declared the funds to U.S. authorities upon arrival to the United States and filed the same FinCEN Form 105. We also note that this reporting requirement would not be triggered by a transfer of funds through normal banking procedures that does not involve the physical transportation of currency or monetary instruments across the U.S. border.

For purposes of this reporting obligation, the term "monetary instruments" does not include checks that bear restrictive endorsements. For example, a check made payable to John Doe and endorsed on the back by Mr. Doe's signature and the words "For Deposit Only" would bear a restrictive endorsement and thus would not be considered a monetary instrument that could trigger this reporting requirement. If, however, the same check is merely endorsed (signed) on the back by Mr. Doe, such document represents a bearer instrument (it could be cashed by anyone in possession of the document) and would be deemed a monetary instrument that could trigger the reporting requirement.

Case Study: **Q.** A customer came to the captive agent's office to pay $15,678 premium on a universal life policy. He took $16,000 in $100 bills out of a duffel bag, with a lot of money still visible in the bag. The bag had a yellow Lufthansa name tag and a white luggage destination tag marked "JFK" still attached, looking like it just came from an airport. He also inquired whether there were any safe deposit boxes nearby that he could rent. The agent took the money and processed his payment. Has the agent done anything wrong?

A. The agent was correct to process the transaction but the insurer will need to file a FinCEN 8300 report for receipt of cash in excess of $10,000 and may also need to file a FinCEN 105 report for transportation of currency.

- The agent should have asked him whether he brought the money into the United States and, if so, whether he reported it to U.S. authorities upon arrival.
- If he brought the money in but did not report it, the insurer (through the agent) has just received more than $10,000 in cash that was physically transported into the United States. The insurer has to report it by filing the FinCEN 105 form.
- In addition, the insurer may need to file a mandatory SAR if customers do not normally pay premiums in cash and/or due to specific circumstances of this case

D. Penalties

In general, penalties for violations of the AML requirements depend on the type of violation and regulatory provision involved, and they may be aggregated (e.g., penalties for failure to file a report, keep records, meet other BSA requirements etc.). Civil penalties are imposed against institutions and/or individual officers or employees for willful (reckless

disregard) and negligent violations (including a "pattern of negligent activity)". These penalties could include:

- $100,000 per willful violation;
- $500 per negligent violation (a pattern of negligent activity could result in an additional fine of up to $50,000); or
- Up to 2 times the amount of the transaction (up to $1 million) for violations of "special measures."

Recent major settlements involving BSA/USA PATRIOT Act violations include penalties of: $10 million by BankAtlantic in April 2006, $30 million by ABN AMRO Bank in December 2005, $2.8 million by Oppenheimer & Co. in December 2005, and $25 million by Riggs Bank in May 2004. 36/

* * * *

In light of the broad scope of OFAC sanctions regulations and AML provisions discussed above, insurance companies need to understand these restrictions and take steps to adhere to the applicable compliance and reporting obligations. Insurance companies also should monitor developments in these areas to ensure ongoing compliance.

36/ In some cases, both OFAC and AML penalties are assessed concurrently; for example, ABN AMRO agreed to pay $40 million, assessed by OFAC and the Federal Reserve, which also satisfies FinCEN's assessed penalty of $30 million.