Santa Clara University
School of Law

Santa Clara Law Review

Volume 53 | Number 1 Article 4

7-25-2013

Financial Counterintelligence: How Changes to the U.S. Anti-Money Laundering Regime Can Assist U.S. Counterintelligence Efforts

Mark B. Skerry

FINANCIAL COUNTERINTELLIGENCE: HOW CHANGES TO THE U.S. ANTI-MONEY LAUNDERING REGIME CAN ASSIST U.S COUNTERINTELLIGENCE EFFORTS

Mark B. Skerry*

TABLE OF CONTENTS

Introduction 206
I. Foreign Intelligence Activities in the United States 211
  A. A General Overview of Intelligence Activities 211
  B. Foreign Intelligence Threats to the United States 212
  C. United States Agencies Engaged in Counterintelligence Activities 215
II. AML Regulations 216
  A. The Crime of Money Laundering 217
  B. International Techniques to Combat Money Laundering Activities 219
    1. Customer Identification and Due Diligence 220
    2. Suspicious Transaction Reporting 222
    3. Cash Transaction Reporting 222
  C. United States-Specific Regulations 223
  D. Suspicious Activity Reports in the United States 225
III. Recommendation: Implement a Foreign Intelligence Detection Program That Builds Upon the Current Anti-Money Laundering Requirements 227
  A. Require Financial Institutions to File Suspicious Activity Reports for Suspected Foreign Intelligence Financial Transactions 228
  B. Promoting Compliance by the Financial Institutions 229
  C. Financial Transaction Typologies That May Suggest Foreign Intelligence Activity 232

* Attorney, U.S. Department of Homeland Security, Office of the General Counsel; J.D. Case Western Reserve University; B.S. Cornell University. Any views or opinions presented in this article are solely those of the author and do not necessarily represent those of the Department of Homeland Security.

1. Client is Employed in an Industry Frequently Targeted by Foreign Intelligence Agencies 233
2. Client Has Poor Credit 234
3. The Transaction Involves a Possible Foreign Intelligence Front Organization 235
Conclusion 237

INTRODUCTION

Along with the proliferation of weapons of mass destruction and international terrorism, the Director of National Intelligence has identified the threat posed by foreign intelligence as one of the top three national security concerns to the United States.[1] There are four million people in the United States with access to classified government information, and they are increasingly targeted by foreign intelligence services interested in obtaining U.S. national security-related information.[2] As noted by the former Central Intelligence Agency (CIA) Associate Deputy Director of Operations for Counterintelligence before the House Permanent Select Committee on Intelligence, the intelligence services of at least forty-one countries are attempting to obtain classified U.S. government secrets.[3] Indeed, Russian intelligence operations in the United States have recently returned to levels seen only during the height of the Cold War.[4]

1. STATEMENT FOR THE RECORD ON THE WORLDWIDE THREAT ASSESSMENT OF THE U.S. INTELLIGENCE COMMUNITY FOR THE HOUSE PERMANENT SELECT COMMITTEE ON INTELLIGENCE 112th Cong. 1, at 3 (2011) (statement of James R. Clapper, Director, National Intelligence), *available at* http://www.dni.gov/files/documents/Newsroom/Testimonies/20110210_testimony_hpsci_clapper.pdf.

2. *See How to Catch a Spy*, TIME MAG., June 21 2005, http://www.time.com/time/magazine/article/0,9171,1074835,00.html.

3. SHARAD S. CHAUHAN, INSIDE C.I.A.: LESSONS IN INTELLIGENCE 357 (2004).

4. Michelle Van Cleave, *Strategic Counterintelligence: What Is It and What Should We Do About It?*, 51 STUD. IN INTELLIGENCE 1, 3 (2007), *available at* https://www.cia.gov/library/center-for-the-study-ofintelligence/csipublications/csi-studies/studies/vol51no2/Studies_v51no2_2007-5Jun.pdf. (stating that "foreign powers increasingly are running intelligence operations with unprecedented independence from their diplomatic establishments. . . . Russia, reversing a sharp decline that took place during the late Boris Yeltsin's presidency, now has an intelligence presence in the United States equal to its Cold War level, a sizing decision presumably indicative of the return on investment.").

For example, the Federal Bureau of Investigation (FBI) in 2010 arrested ten illegals—spies clandestinely inserted into the United States by foreign intelligence services—for conducting intelligence operations on behalf of Russia's primary external intelligence service—the SVR.[5] The illegals spent years, and in some cases decades, developing fake identities in the United States while attempting to collect intelligence for Russia and awaiting orders on future targets.[6] While the arrests are certainly an accomplishment for U.S. counterintelligence officials, this one network of illegals pales in comparison to the pervasiveness of possible foreign intelligence operations ongoing in the United States. Sergei Tretyakov, the Russian intelligence officer responsible for SVR operations in New York City from 1995 to 2005, revealed that at one point he was in charge of sixty SVR officers in addition to "160 contacts made up of illegals, outright spies, and other people who knowingly or unknowingly could supply information useful to Russia."[7] These figures are troubling—they represent the activities of just one spy ring, from just one foreign intelligence service, in just one U.S. city.

Another concern within the counterintelligence community is the growing threat of economic and industrial espionage.[8] Foreign intelligence services are increasingly seeking out information about sensitive technologies beyond traditional military and government secrets.[9] For example, the Chinese government has developed a "pervasive

5. Walter Pincus, *Fine Print: Despite Arrests, Russian 'Illegals' Won't Go Away*, WASH. POST, July 13, 2010, http://www.washingtonpost.com/wp-dyn/content/article/2010/07/12/AR2010071205341.html.

6. Ellen Barry, *'Illegals' Spy Ring Famed in Lore of Russian Spying*, N.Y. TIMES, June 29, 2010, http://www.nytimes.com/2010/06/30/world/europe/30sleepers.html.

7. Pincus, *supra* note 5.

8. OFFICE OF THE NAT'L COUNTERINTELLIGENCE EXEC. (ONCIX), ANNUAL REPORT TO CONGRESS ON FOREIGN ECONOMIC COLLECTION AND INDUSTRIAL ESPIONAGE, FY 2008, at iii (2009), *available at* http://www.ncix.gov/publications/reports/fecie_all/fecie_2008/2008_FECIE_Blue.pdf. Economic espionage is the "knowing misappropriation of trade secrets with the knowledge or intent that the offense will benefit a foreign government, foreign instrumentality, or foreign agent. Misappropriation includes, but is not limited to, stealing, copying, altering, destroying, transmitting, sending, receiving, buying, possessing, or conspiring to obtain trade secrets without authorization." *Id.* at v. Examples of trade secrets include "financial, business, scientific, technical, economic, or engineering information." *Id.*

9. *See id.* at iii.

intelligence and security apparatus" that exploits the large number of Chinese nationals traveling to the United States seeking education and employment.[10] The Deputy Director of the FBI for Counterintelligence recently noted that there are approximately 3200 Chinese front companies in the United States operating for the sole purpose of gaining proprietary information and sensitive technologies.[11] For example, the Department of Justice recently filed economic espionage charges against five individuals and five companies controlled by the People's Republic of China for the theft of titanium dioxide production technologies from E.I. du Pont de Nemours and Company (commonly referred to as DuPont).[12] And China is not alone in this effort. The FBI stated that at least one hundred countries are attempting to purchase sensitive U.S. technologies, and fifty-seven of those countries are actively "engaging in covert operations against U.S. corporations."[13] Apart from China, the most aggressive offenders noted by the FBI include France, Israel, Russia, Iran, Cuba, the Netherlands, Belgium, Germany, Japan, Canada, India, and several Scandinavian countries.[14]

This paper proposes a novel weapon to combat the rising tide of foreign intelligence threats: expansion of the U.S. Anti-Money Laundering (AML) regime to uncover financial transactions related to foreign intelligence. Under current U.S. AML laws, all financial institutions must monitor the identities and financial transactions of their clients.[15] Throughout this process, the institutions are required to create a "profile" for all clients, and monitor their transactions to ensure that the transactions are considered

10. Larry M. Wortzel, *Risks and Opportunities of a Rising China*, THE HERITAGE FOUND., 6 (Jun. 22, 2006), *available at* http://s3.amazonaws.com/thf_media/2006/pdf/hl948.pdf.

11. *Id.*

12. U.S. DEP'T OF JUSTICE, OFFICE OF PUB. AFFAIRS, U.S. AND CHINESE DEFENDANTS CHARGED WITH ECONOMIC ESPIONAGE AND THEFT OF TRADE SECRETS IN CONNECTION WITH CONSPIRACY TO SELL TRADE SECRETS TO CHINESE COMPANIES (2012), *available at* http://www.justice.gov/opa/pr/2012/February/12-nsd-180.html.

13. HEDIEH NASHERI, ECONOMIC ESPIONAGE AND INDUSTRIAL SPYING 8 (2005).

14. *See id.*

15. 31 U.S.C. § 5318(l) (2011); *see also* 31 C.F.R. § 103.121 (2010); 31 C.F.R. § 103.18(a)(2).

normal for that individual's profile.[16] The financial institution must report any unusual activity, such as an unexplained cash deposit, to the federal government.[17] This paper argues that financial institutions could alter their AML programs to detect transactions that may suggest foreign intelligence activity. A U.S. government employee makes an unusual cash deposit in addition to his current wages. A foreign national opens a bank account with suspicious documentation and then receives regular wire transfers from his home country, or from his home country traced through an overseas third party. A corporation within the U.S. defense industry engages in a transaction with a foreign shell corporation for no apparent business purpose. Each of these isolated situations may never catch the attention of counterintelligence officials working in the United States. Under this proposal, however, such transactions could trigger AML suspicion and be reported to the federal government by financial institutions.

Although financial institutions may already identify some of these transactions as traditional money laundering or terrorism finance efforts and report them to the federal government under the current AML regime, there are three reasons why change is needed. First, the agency that receives reports of suspicious activity—the Financial Crimes Enforcement Network (FinCEN)—is woefully underfunded for the number of reports it already receives.[18] As such, it has prioritized analysis of those reports that deal primarily with terrorism finance.[19] Suspicious transactions suggesting foreign intelligence activity that would otherwise go unnoticed could be forwarded immediately to counterintelligence elements of U.S. intelligence agencies for further investigation.

Second, FinCEN has focused its resources on developing typologies specific to general money laundering activity and

16. *See* 31 U.S.C. § 5318(a); 31 C.F.R. § 103.121.

17. 31 C.F.R. § 103.18.

18. *See* FIN. ACTION TASK FORCE (FATF), SUMMARY OF THE THIRD MUTUAL EVALUATION REPORT ON ANTI-MONEY LAUNDERING AND COMBATING THE FINANCING OF TERRORISM: UNITED STATES OF AMERICA 3 (2006), *available at* http://www.treasury.gov/resource-center/international/standards-codes/Documents/mer-executive-summary.pdf.

19. *Id.*

terrorism finance.[20] A typology describes "typical tactics used by launderers or patterns that indicate a higher risk of laundering,"[21] and are provided to financial institutions so that the institution actually understands what a suspicious transaction would look like.[22] At the present time, no concerted effort has been made to develop typologies that would suggest foreign intelligence activity.[23] Thus, financial institutions are unable to identify many transactions that could suggest such activity.

Third, the pervasive threat that foreign intelligence operations pose to the United States warrants heightened scrutiny of those with access to classified information and sensitive technologies. Financial institutions should be required to expand their due diligence efforts of clients working within the federal government and within industries with access to sensitive U.S. technologies.

Part I of this Article discusses foreign intelligence activities and the threats they pose to U.S. security interests. Part II discusses the current anti-money laundering regime and the methods used to uncover illegal activity. Part III advocates changes to the AML system necessary to identify foreign intelligence activity. It also discusses potential issues with compliance by financial institutions, and the need for additional counterintelligence community discussions on potential indicators and typologies for identifying transactions that suggest foreign intelligence activity.

20. *See id.*

21. Richard K. Gordon, *Trysts of Terrorists? Financial Institutions and the Search for Bad Guys*, 43 WAKE FOREST L. REV. 699, 726 (2008).

22. *See* PAUL ALLAN SCHOTT, THE WORLD BANK, REFERENCE GUIDE TO ANTI-MONEY LAUNDERING AND COMBATING THE FINANCING OF TERRORISM I-10 (2d ed. 2006) ("The various techniques used to launder money or finance terrorism are generally referred to as *methods* or *typologies*.").

23. For example, FATF's most recent Global Money Laundering & Terrorist Financing Threat Assessment provides an "overview of the systemic money laundering (ML) and terrorist financing (TF) threats and ultimate harms that they can cause." FIN. ACTION TASK FORCE (FATF), GLOBAL MONEY LAUNDERING & TERRORIST FINANCING THREAT ASSESSMENT 3 (2010), http://www.fatfgafi.org/media/fatf/documents/reports/Global%20Threat%20assessment.pdf. An extensive list of money laundering typologies and recommended financial countermeasures is provided in Annex D. The document does not offer any guidance on money laundering activities specific to the counterintelligence field. *See id.* at 69–75.

I. FOREIGN INTELLIGENCE ACTIVITIES IN THE UNITED STATES

A. A General Overview of Intelligence Activities

At the most basic level, intelligence activities offer "a particular kind of information that helps to inform, instruct, and educate the policy world."[24] Intelligence missions generally fall into one of three categories: (1) collection and analysis, (2) counterintelligence, or (3) covert action.[25] The first form of intelligence—collection and analysis—focuses on gathering information from technical sources (TECHINT),[26] signals intelligence (SIGINT),[27] human sources (HUMINT), and open-source literature (OSINT).[28] Once this information is collected, it is amassed and processed by intelligence officers to offer insight to relevant geopolitical issues.[29] This new information is then disseminated to policymakers.[30]

The second type of intelligence mission—counterintelligence—comprises those activities intended to defeat foreign intelligence officers collecting information.[31] For example, Executive Order 12333 defines counterintelligence, in part, as "information gathered and activities conducted to protect against espionage, other intelligence activities, sabotage, or assassinations conducted for or on behalf of foreign powers, organizations or persons, or international terrorist activities."[32] This can include both the discovery of moles within the country's own intelligence

24. MICHAEL A. TURNER, WHY SECRET INTELLIGENCE FAILS 3 (2005). Turner defines intelligence as "policy-relevant information, collected through open and clandestine means and subjected to analysis, for the purposes of educating, enlightening, or helping American decision makers in formulating and implementing national security and foreign policy." *Id.* at 4.

25. Loch K. Johnson, *An Introduction to the Intelligence Studies Literature*, *in* STRATEGIC INTELLIGENCE 1: UNDERSTANDING THE HIDDEN SIDE OF GOVERNMENT 1, 4 (Loch K. Johnson ed., 2007).

26. *Id.* TECHINT could include images from satellites and reconnaissance planes. *Id.*

27. *Id.* SIGINT is the interception of signals such as telephone conversations or electronic communications. *See id.*

28. *Id.* OSINT could include information from newspapers or public speeches. *Id.*

29. *Id.* at 5.

30. *Id.*

31. *See id.* at 6.

32. Exec. Order No. 12333 § 3.4(a), 46 Fed. Reg. 59941 (Dec. 4, 1981).

services[33] and foreign intelligence assets working within the country.[34] However, counterintelligence efforts also include providing personnel security, protecting information that counterintelligence officials believe foreign governments would be interested in obtaining, and misleading and misdirecting foreign spies away from the country's real secrets.[35]

Covert action, the third type of intelligence mission, is activity intended to "secretly influence and manipulate events abroad."[36] These activities can include "the use of propaganda, political activities, economic disruption, and paramilitary operations."[37] In the United States, covert activities have included the Bay of Pigs operation in 1961 and the Iran-*contra* affair in 1986.[38] While the U.S. Intelligence Community is actively engaged in each of these efforts, this Article focuses on the second: defeating foreign intelligence activities adverse to U.S. interests.

B. Foreign Intelligence Threats to the United States

The "treasure trove" of U.S. information targeted by foreign intelligence threats lies within the United States.[39] This is because foreign intelligence officers are primarily concerned with three things: (1) the organizations and individuals responsible for setting American policy; (2) the research and development efforts of U.S. weapons, nuclear, and technological enterprise industries; and (3) the facilities and employees engaged in classified national security efforts.[40] U.S. activity in these three areas is primarily conducted domestically; thus, the majority of foreign intelligence threats are engaged in activity within U.S.

33. Some of the best sources of intelligence are citizens of the target country. KATHERINE L. HERBIG & MARTIN F. WISKOFF, DEF. PERSONNEL SEC. RESEARCH CTR., ESPIONAGE AGAINST THE UNITED STATES BY AMERICAN CITIZENS 1947–2001, at 1 (2002), *available at* http://www.dhra.mil/perserec/reports/tr02-05.pdf.

34. *See* TURNER, *supra* note 24, at 126.

35. *Id.*

36. Johnson, *supra* note 25, at 7.

37. *Id.* at 4.

38. *Id.* at 7.

39. Van Cleave, *supra* note 4, at 3.

40. *See id.*

borders.[41]

In the intelligence community, there are two types of foreign intelligence case officers that travel to the United States: those who operate under diplomatic or official "cover," and those who do not.[42] Intelligence officers working under official cover enter the United States as a member of the country's diplomatic corps or as a military liaison.[43] This employment is a pretense; they are provided a cover story and normal identification cards, but actively engage in intelligence collection activities in that target country.[44] Historically, U.S. counterintelligence efforts have focused on "embassies and other diplomatic establishments . . . because of the operational security they afford."[45] As such, the United States can usually identify these spies without issue; routine surveillance can easily be conducted on foreigners working in embassies within the United States.[46]

However, some foreign intelligence case officers work under "nonofficial cover," meaning they have no official connections with their home country's government.[47] These officers typically work in commercial or private enterprises as a pretense, engaging in intelligence collection activities on the side for their home country.[48] These nonofficial cover agents are sometimes referred to as "illegals."[49] Foreign governments secretly insert these illegals into the United States making it hard to identify them because they "masquerade as ordinary Americans."[50]

In recent years, globalization has promoted the use of the illegals technique. A former U.S. National Counterintelligence Executive notes that "we have seen a growing number of intelligence operations within our borders, facilitated by an extensive foreign presence that provides

41. *Id.* at 4 n.d ("Three-quarters of the U.S. [counterintelligence] budget since World War II has been devoted to activities within the United States . . . .").
42. *See* TURNER, *supra* note 24, at 90–91.
43. *Id.* at 90.
44. *See id.* at 91.
45. Van Cleave, *supra* note 4, at 3.
46. *See* TURNER, *supra* note 24, at 132.
47. *See id.* at 91.
48. *See id.*
49. *Id.* at 132.
50. *Id.*

cover for intelligence services and their agents."[51] She continued:

> Foreign powers increasingly are running intelligence operations with unprecedented independence from their diplomatic establishments. The number of formal and informal ports of entry to the country, the ease with which people can travel internally, and the relatively benign operational environment of the United States are tailor made for embedded clandestine collection activities. Thousands of foreign owned commercial establishments in the United States, the routine interactions of trade and transnational business and finance, and the exchange of hundreds of thousands of students and academicians, all potentially extend the reach of foreign intelligence into the core structures of our nation's security.[52]

In this globalized world, there is now even a "market" for U.S. national security-related information.[53] Indeed, counterintelligence officials believe that the intelligence services of at least forty-one countries are attempting to obtain classified U.S. government secrets.[54]

Of great concern is the fact that illegals have increasingly targeted U.S. economic and commercial secrets.[55] Under attack are corporations, research centers, and universities.[56] In FY 2007, the FBI opened fifty-five new cases of economic espionage and continued investigations of another eighty-eight cases.[57] In FY 2008, Immigrations and Customs Enforcement arrested 158 individuals on charges related to the exportation of sensitive U.S. technologies.[58] In that same time period, the Department of Commerce investigated an

51. Van Cleave, *supra* note 4, at 3.

52. *Id.* at 3.

53. *Id.* at 2; *see also* RICHARD A. BEST, CONG. RESEARCH SERV., R41848, INTELLIGENCE INFORMATION: NEED-TO-KNOW VS. NEED-TO-SHARE 12 (2011) ("Foreign countries (including friendly ones or even allies) may not turn down opportunities to gain insight into U.S. policymaking or military capabilities. Various anti-American organizations worldwide eagerly seek information that can damage or embarrass the U.S. Government. Major media outlets, not all of which are in foreign countries, consider themselves free to publish classified information regardless of possible damage to U.S. persons, interests, or foreign supporters. There is, in short, an active market for classified information . . . .").

54. CHAUHAN, *supra* note 3, at 357.

55. TURNER, *supra* note 24, at 132.

56. *Id.*

57. ONCIX, *supra* note 8, at 1.

58. *Id.*

additional 792 export violations.[59] Individuals arrested for economic and industrial espionage against the United States have come from countries including China, Cuba, India, and Iran.[60] However, evidence suggests that fifty-seven nations are actively engaging in covert activity against U.S. corporations, and forty-three more are attempting to purchase sensitive U.S. technologies.[61] While the United States has focused the majority of its counterintelligence assets on threats to government secrets, recent trends have required it to shift some of these resources to protecting commercial secrets.[62]

Both types of foreign intelligence officers—cover and nonofficial cover agents—also actively seek to recruit Americans whose employment offers them access to secret information.[63] In fact, most illegals enter the country to gather information on those who could potentially be turned as spies, foregoing opportunities to collect information themselves.[64] The problem is pervasive; the U.S. government has caught and convicted over one thousand American citizens for acts of espionage since World War II.[65]

The first step in thwarting foreign intelligence activities is to identify who the foreign intelligence assets are.[66] While U.S. counterintelligence may have a good grasp on the identities of official cover agents working in the United States, more hidden are the illegals and the Americans committing espionage.[67] Uncovering these hidden spies and their cover organizations is a primary goal for U.S. counterintelligence officials, and is the focus of this Article.

C. United States Agencies Engaged in Counterintelligence Activities

The majority of counterintelligence activity conducted by the United States is shared between the FBI, CIA, and

59. *Id.*
60. *See id.* app. B, at 9–12.
61. *See* NASHERI, *supra* note 13, at 8.
62. *See* TURNER, *supra* note 24, at 127.
63. *See* Van Cleave, *supra* note 4, at 3.
64. *See* Pincus, *supra* note 5.
65. TURNER, *supra* note 24, at 134.
66. *See id.* at 132.
67. *Id.*

Department of Defense.[68] The CIA is generally responsible for those counterintelligence activities outside U.S. borders.[69] Within the United States, the CIA counterintelligence team is tasked only with the security of its own employees unless working in conjunction with the FBI.[70] Some departments and agencies have specialized counterintelligence units, with mission-specific objectives. For example, the Department of Defense has counterintelligence units throughout its branches and within its Defense Intelligence Agency (DIA).[71] But the lion's share of domestic counterintelligence activity falls to the FBI.[72] In fact, three-fourths of all money spent on U.S. counterintelligence efforts since World War II has been on the FBI's domestic counterintelligence program.[73]

During the 1990s, President Clinton formed both the National Counterintelligence Center (NCIC) and the National Counterintelligence Executive (NCIX) to provide a cohesive approach to U.S. counterintelligence efforts.[74] However, commentators note that both organizations have been ineffective in this regard, leaving much of the counterintelligence decision-making with individual agencies.[75]

II. AML REGULATIONS

To understand how the AML regime can be applied to counterintelligence activity, it is important first to understand the crime of money laundering, the international standards that led to AML efforts within the United States, and the specific U.S. laws that implement these international standards.

68. *See id.* at 36.

69. Exec. Order No. 12333 §§ 1.8(a)–(d), 46 Fed. Reg. 59941 (Dec. 4, 1981); *see also* TURNER, *supra* note 24, at 99.

70. Exec. Order No. 12333 §§ 1.8(a), (h), 46 Fed. Reg. 59941 (Dec. 4, 1981); *see also* TURNER, *supra* note 24, at 36.

71. *See* TURNER, *supra* note 24, at 28–30; Van Cleave, *supra* note 4, at 2.

72. *See* 50 U.S.C. § 402a(e) (2005) ("Coordination of counterintelligence matters with Federal Bureau of Investigation."); *see also* TURNER, *supra* note 24, at 99.

73. Van Cleave, *supra* note 4, at 4 n.d.

74. TURNER, *supra* note 24, at 127.

75. *See id.* at 127–28; Van Cleave, *supra* note 4, at 1–2.

A. The Crime of Money Laundering

Money laundering is "the process by which proceeds from a criminal activity are disguised to conceal their illicit origins."[76] A predicate offense is criminal activity that generates proceeds, which when laundered, leads to the crime of money laundering.[77] While the international community's first attempts to criminalize the act of money laundering focused on crimes related to drug trafficking,[78] later treaties require countries to criminalize money laundering to "the widest range of predicate offenses."[79]

As a hypothetical, Donny Dealer sells one thousand dollars' worth of drugs to his neighbor. Donny takes that cash, enters a casino, and trades the cash for chips. He gambles for a few minutes and then redeems the chips at the casino, but asks the casino to deposit the money into his bank account. Donny now has about one thousand dollars in his bank account and, if questioned about the origins of this money, can claim that he won all of it at the casino. He then uses that money to purchase a used moped, perhaps to expand his customer base. The predicate offense in this example would be the sale of illegal narcotics. But, Donny would also be culpable for the crime of money laundering, because he took the proceeds of his crime and attempted to disguise their illicit origins.

Money laundering activities generally include three stages: placement, layering and integration.[80] Following the generation of proceeds of crime, money laundering

76. SCHOTT, *supra* note 22, at I-1 (emphasis omitted).

77. *Id.* at I-3.

78. *See* United Nations Convention Against Illicit Traffic in Narcotic Drugs and Psychotropic Substances, 1998, Dec. 19, 1988, 28 I.L.M. 493, *available at* http://www.unodc.org/pdf/convention_1988_en.pdf.

79. *See* SCHOTT, *supra* note 22, at I-3 (quoting United Nations Convention Against Transnational Organized Crime (Palermo Convention), art. 6(2)(a) (2000), *available at* http://www.uncjin.org/Documents/Conventions/dcatoc/final_documents_2/convention_eng.pdf). For example, the United States has classified all Racketeer Influenced and Corrupt Organization (RICO) predicate offenses, such as murder, kidnapping, and extortion, as well as numerous other federal crimes, as money laundering predicate offenses. CHARLES DOYLE, CONG. RESEARCH SERV., RS22401, MONEY LAUNDERING: AN ABRIDGED OVERVIEW OF 18 U.S.C. 1956 AND RELATED FEDERAL CRIMINAL LAW 2 (2012). For a comprehensive list of predicate offenses in the United States, see 18 U.S.C. § 1956(c)(7) (2012).

80. SCHOTT, *supra* note 22, at I-7.

commences with the placement of the proceeds into the financial system.[81] The primary purpose of this step is to introduce "dirty" money into the system "without attracting the attention of financial institutions or law enforcement."[82] This can be a deposit at a bank, a purchase of an asset like an automobile, the exchange of currency, or the conversion into financial instruments such as money orders or checks.[83] In our example, Donny Dealer engaged in placement of his illegal proceeds when he exchanged the cash for casino chips.

Following placement, the money launderer will engage in layering.[84] Layering can include a range of activities such as moving or selling the bank deposits, financial instruments, or purchased assets to different financial institutions.[85] The money launderer may use overseas shell corporations in this step, may hide the transfer as a payment for goods or services, or may merely transfer the placed money among several banks.[86] The purpose of this step is to "create confusion and complicate the paper trail."[87] Donny Dealer engaged in placement activities when he cashed in his casino chips and transferred his "winnings" to his bank account.

Finally, the money launderer must engage in integration.[88] This involves integrating the funds back into the legitimate economy.[89] It is often accomplished by purchasing an asset such as real estate, securities, or luxury goods.[90] The purpose of doing so would be to provide the criminal with a "plausible explanation for the source of the funds."[91] Donny Dealer integrated his proceeds of crime back into the legitimate economy by purchasing the moped. He now has legitimate title to the vehicle and can use it or sell it without raising suspicion.

81. *Id.*

82. FED. FIN. INST. EXAMINATION COUNCIL (FFIEC), BANK SECRECY ACT/ANTI-MONEY LAUNDERING EXAMINATION MANUAL 12 (2010), *available at* http://www.ffiec.gov/bsa_aml_infobase/documents/BSA_AML_Man_2010.pdf.

83. *See* SCHOTT, *supra* note 22, at I-7.

84. *Id.* at I-8.

85. *Id.*

86. *Id.* at I-8–I-9.

87. FFIEC, *supra* note 82, at 12.

88. SCHOTT, *supra* note 22, at I-9.

89. *Id.*

90. *Id.*

91. FFIEC, *supra* note 82, at 12.

B. International Techniques to Combat Money Laundering Activities

Countries that implement effective techniques to combat money laundering see significant benefits to their economies.[92] Anti-money laundering efforts can assist in fighting crime and corruption,[93] enhance the stability of financial institutions,[94] and encourage economic development.[95] In order to develop an international response to money laundering, the G-7 countries formed the Financial Action Task Force on Money Laundering (FATF) in 1989.[96] FATF adopted "Forty Recommendations," which are now regarded as the relevant international standard for AML.[97] Any country desiring to comply with international AML standards must implement laws in its own country that fulfill these Forty Recommendations.[98] While the Forty Recommendations cover a wide range of legal requirements, the most pertinent to counterintelligence activities are those pertaining to prevention and discovery of money laundering activity.

92. *See* SCHOTT, *supra* note 22, at II-7.

93. *See id.* ("When money laundering itself is made a crime, it provides another avenue to prosecute criminals, both those who commit the underlying criminal acts and those who assist them through laundering illegally obtained funds. Similarly, an [AML] framework that includes bribery as a predicate offense and is enforced effectively provides fewer opportunities for criminals to bribe or otherwise corrupt public officials.").

94. *Id.* at II-8 ("Public confidence in financial institutions, and hence their stability, is enhanced by sound banking practices that reduce financial risks to their operations.").

95. *See id.* at II-8–II-9 ("Money laundering has a direct negative effect on economic growth by diverting resources to less productive activities. . . . Rather than being placed in productive channels for further investment, laundered funds are often placed into 'sterile' investments to preserve their value or make them more easily transferable. . . . Even worse, criminal organizations may transform productive enterprises into sterile investments by operating them for the primary purpose of laundering illegal proceeds, rather than as profit-generating enterprises.").

96. *Id.* at III-7. G-7 countries include Canada, France, Germany, Italy, Japan, the United Kingdom, and the United States. *Id.* at III-7 n.30. FATF later also assumed responsibilities for combating the financing of terrorism. *Id.* at III-8.

97. *Id.* at III-9.

98. *See id.*

1. Customer Identification and Due Diligence

The first AML prevention technique required by FATF involves customer identification and due diligence. More commonly known as Know-Your-Customer (KYC) rules,[99] this group of recommendations requires countries to implement laws that place duties on banking and financial institutions to keep detailed records on their customers.[100] To this end, financial institutions must at all times verify the true identities of their clients.[101] Where the client is a legal entity, such as a corporation, the financial institution must take reasonable steps to determine the true parent company and owner of the client.[102] Where the institution has reason to believe that the client is acting on behalf of a third party, the financial institution should take similar due diligence measures to verify the identity of this third-party beneficiary.[103]

Institutions must also collect information on the nature of the business relationship it will have with the client.[104] Using this information, the institution must create a profile for each client so that the institution can understand what financial transactions would be normal for that client.[105] The institution is required to conduct ongoing due diligence in light of this profile, scrutinizing the client's transactions to ensure that they are "consistent with the institution's knowledge of the customer, their business and risk profile, including, where necessary, the source of funds."[106]

Returning to the previous example, when Donny Dealer opened his bank account, he had to provide documentation to

99. *Id.* at VI-3 & n.6 (citing BASEL COMM., CORE PRINCIPLE FOR EFFECTIVE BANKING SUPERVISION, PRINCIPLE 15 (1997) as the origin of the term "know-your-customer").

100. FIN. ACTION TASK FORCE (FATF), 40 RECOMMENDATIONS 4–7 (2010), *available at* http://www.fatf-gafi.org/media/fatf/documents/FATF%20Standards%20-%2040%20Recommendations%20rc.pdf; SCHOTT, *supra* note 22, at VI-2.

101. FATF, *supra* note 100, at 4–5.

102. *Id.* at 5; SCHOTT, *supra* note 22, at VI-4 ("When corporations or legal entities are involved, appropriate due diligence measures should be employed to determine the identity of the actual parent or controlling entity.").

103. FATF, *supra* note 100, at 5; SCHOTT, *supra* note 22, at VI-4 ("If there is any reason to suspect that the customer is acting on behalf of another person or entity, appropriate due diligence measures should be instituted.").

104. FATF, supra note 100, at 5.

105. *See id.*

106. *Id.*

prove his identity, and when asked about his profession, Donny informed the bank that he was a law professor. As a law professor, the bank would expect to see a salary paid into his account on a regular basis, as these transactions would be typical for a law professor. If Donny were to deposit one million dollars cash in small bills over the course of a year, this would raise red flags at Donny's bank, and the bank would need to investigate further and perhaps even report the transactions to the government. In contrast, Donny's neighbor, Gus, owns a gas station. If Gus were to deposit one million dollars cash in small bills into his bank account over the course of one year, the bank may consider this normal in light of Gus's business, and forego further scrutiny.

Certain types of risky clients automatically warrant heightened scrutiny under FATF's recommendations because FATF considers them more likely to engage in money laundering activities.[107] For example, clients that are classified as Politically Exposed Persons (PEP) require heightened due diligence.[108] FATF defines PEPs, in part, as "individuals who are or have been entrusted with prominent public functions in a foreign country."[109] Examples of PEPs include Heads of State, senior government officials or politicians, members of a country's judiciary, and high-ranking military officials.[110] Risky clients may also include foreigners, legal persons such as trusts that are merely personal asset holding vehicles, and companies that have nominee shareholders or shares in bearer form.[111]

Certain transactions also warrant heightened due diligence.[112] Recommendation eleven requires financial institutions to afford increased scrutiny to "all complex, unusual large transactions, and all unusual patterns of transactions, which have no apparent economic or visible

107. FIN. ACTION TASK FORCE (FATF), METHODOLOGY FOR ASSESSING COMPLIANCE WITH THE FATF 40 RECOMMENDATIONS AND THE FATF 9 SPECIAL RECOMMENDATIONS 17 (2009), *available at* http://www.fatf-gafi.org/media/fatf/documents/reports/methodology.pdf ("Financial institutions should be required to perform enhanced due diligence for higher risk categories of customer, business relationship or transaction.").

108. *See* FATF, *supra* note 100, at 5–6.

109. *Id.* at 17.

110. *Id.*

111. FATF, *supra* note 107, at 17.

112. FATF, *supra* note 100, at 7.

lawful purpose."[113] The Recommendation requires the institution to ascertain, "as far as possible," the circumstances and purpose of the transaction.[114] Institutions should document the findings in writing and make them available to law enforcement authorities.[115]

2. Suspicious Transaction Reporting

Upon discovery of any transaction that appears to involve money laundering, a financial institution must report that information to its country's Financial Intelligence Unit (FIU).[116] When determining which transactions involve money laundering, financial institutions must rely upon the risk profiles created for each account and create systems that screen transactions for abnormal activity.[117] Financial institutions need not have evidence that the client is engaged in money laundering before it reports the transaction to its FIU.[118] Instead, institutions must merely have "'suspicion' that funds may be related to a criminal offense."[119]

In Donny Dealer's case, it probably would not be abnormal for a law professor to win one thousand dollars at a casino; therefore, Donny's bank probably would not report the transfer of those funds from the casino. The casino, however, may find it suspicious if Donny trades cash for chips, and then trades in the chips for a bank deposit shortly after. This may rise to the level of abnormality that would require the casino to report the transaction to its country's FIU.

3. Cash Transaction Reporting

While not a requirement for a country to remain in compliance with international AML standards, FATF

113. *Id.*
114. *Id.*
115. *Id.*
116. *Id.* at 8.
117. SCHOTT, *supra* note 22, at VI-19 (noting that any of the following may require further investigation: "[a]ssets withdrawn immediately after they are credited to an account," "[a] dormant account suddenly becomes active without any plausible reason," "[t]he high asset value of a client is not compatible with either the information concerning the client or the relevant business," "[a] client provides false or doctored information or refuses to communicate requiring information to the bank," and "[t]he arrangement of a transaction either insinuates an unlawful purpose, is economically illogical or unidentifiable.").
118. *Id.* at VI-21.
119. *Id.*

recommends that countries implement laws requiring cash transaction reporting.[120] Specifically, this would require financial institutions to report any transaction involving cash or its functional equivalent in an amount greater than the threshold level set by that country.[121]

Of course, these threshold levels are known by criminals as well. Therefore, FATF recommends that financial institutions aggregate all cash transactions conducted over the course of a certain time period, such as one day, to ensure that the client cannot avoid reporting requirements by engaging in many small transactions instead of one big transaction.[122] Furthermore, financial institutions may find suspicious those cash transactions that are just below the reporting threshold, and the financial institution may report the transaction to its FIU regardless.[123]

C. United States-Specific Regulations

The Bank Secrecy Act of 1970 (BSA) and the Money Laundering Control Act of 1986, both as amended by the USA PATRIOT Act of 2002, implement the United States' AML measures as required by the FATF recommendations.[124] Under this regime, all financial institutions are required to implement AML systems which must include "the development of internal policies, procedures and controls," "the designation of a compliance officer," "an ongoing employee training program," and "an independent audit function to test programs."[125] The financial institution must implement a Customer Identification Program (CIP) that includes risk-based procedures that "enable the bank to form a reasonable belief that it knows the true identity of each customer."[126] Furthermore, heightened due diligence must be

120. *See* FATF, *supra* note 100, at 7–8.

121. SCHOTT, *supra* note 22, at VI-24.

122. *Id.* at VI-25.

123. *Id.*

124. U.S. S. PERMANENT SUBCOMM. ON INVESTIGATIONS, MONEY LAUNDERING AND FOREIGN CORRUPTION: ENFORCEMENT AND EFFECTIVENESS OF THE PATRIOT ACT 9, (2004), *available at* http://hsgac.senate.gov/public/_files/ACF5F8.pdf; FATF, *supra* note 18, at 3.

125. 31 U.S.C. § 5318(h)(1) (2011); FATF, *supra* note 18, at 5.

126. 31 C.F.R. § 103.121(b)(2) (2010). See *id.* for a comprehensive list of all procedures financial institutions must implement to comply with U.S. CIP requirements.

observed for foreign financial institutions and wealthy foreign individuals.[127]

Where a financial institution in the United States uncovers a suspicious transaction, that financial institution must report it to the U.S. FIU: FinCEN.[128] The United States created FinCEN in 1990, under the umbrella of the U.S. Treasury Department.[129] FinCEN does not investigate financial crimes, but serves as a "central source for financial intelligence information and analysis."[130] It has primary responsibility over all AML reports filed in the United States.[131] Unfortunately, the sheer number of Suspicious Activity Reports (SARs) filed by financial institutions prevents effective analysis and review of each one.[132] In 2004, FinCEN received over fourteen million reports, including 600,000 SARs.[133] Accordingly, FinCEN has prioritized those reports most valuable to law enforcement, such as those directly related to terrorism finance.[134]

In particular, a bank must report a transaction that is more than five thousand dollars and where the bank "knows, suspects, or has reason to suspect that:" (1) the transaction involves the proceeds of crime; (2) the transaction is "designed to evade" AML rules and reporting requirements; or (3) the transaction "has no business or apparent lawful purpose or is not the sort in which the particular customer would normally be expected to engage, and the bank knows of no reasonable explanation for the transaction after examining the available facts, including the background and possible purpose of the transaction."[135] The bank must file a government-issued SAR form within thirty calendar days of discovering the suspicious nature of the transaction.[136] For obvious reasons, the employees of the notifying institution may not disclose that

127. 31 U.S.C. § 5318(i).
128. *See id.* at (g).
129. FATF, *supra* note 18, at 3.
130. U.S. GOV'T ACCOUNTABILITY OFFICE, GAO-10-141, ANTI-MONEY LAUNDERING: IMPROVED COMMUNICATION COULD ENHANCE THE SUPPORT FINCEN PROVIDES TO LAW ENFORCEMENT 6 (2009), *available at* http://www.gao.gov/new.items/d10141.pdf.
131. *See* FATF, *supra* note 18, at 3.
132. *See id.*
133. *Id.*
134. *Id.*
135. 31 C.F.R. § 103.18(a)(2) (2010).
136. *Id.* at (b)(3).

such a report was made to anyone involved in the transaction.[137]

The BSA also implemented rules for cash transaction reporting in the United States. Financial institutions must keep a record and report any transaction using cash or bearer instruments in excess of $10,000.[138] These reports are compiled into a computerized database and shared with all law enforcement agencies involved in AML activities,[139] such as the FBI, the Drug Enforcement Agency, Immigration and Customs Enforcement, and the U.S. Secret Service.[140]

D. Suspicious Activity Reports in the United States

The most recent version of the U.S. SAR form can be found on FinCEN's website.[141] Part I of the form asks for information identifying the financial institution, such as its name, address, and Federal Tax Identification Number.[142] Part II of the form requires extensive identifying information about the suspect, including his or her name, address, social security or tax identification number, contact information, occupation, date of birth, and relationship to the institution.[143]

Part III asks in-depth questions about the nature of the suspicious activity being reported.[144] Required information includes the total dollar amount involved, the dates that the transaction took place, and those law enforcement agencies that might have already been notified.[145] Part III also includes a question asking the financial institution to characterize the nature of the suspicion using a series of checkboxes.[146] The checkboxes are labeled "a" through "u," and include such characterizations as "Bank Secrecy

137. 31 U.S.C. § 5318(g)(2) (2011).
138. SCHOTT, *supra* note 22, at VI-24.
139. FATF, *supra* note 18, at 4.
140. *See* FIN. CRIMES ENFORCEMENT NETWORK (FINCEN), 14 THE SAR ACTIVITY REV. 1, n.1 (2008).
141. *See* FIN. CRIMES ENFORCEMENT NETWORK (FINCEN), SUSPICIOUS ACTIVITY REPORT (Mar. 2011), *available at* http://www.fincen.gov/forms/files/f9022-47_sar-di.pdf.
142. *Id.*
143. *Id.*
144. *Id.*
145. *Id.*
146. *Id.*

Act/Structuring/Money Laundering," "Bribery/Gratuity," "Computer Intrusion," "Credit Card Fraud," "Defalcation/Embezzlement," and "Identity Theft," among others.[147] Thus, the form is used to report more than just money laundering.[148] Following the USA PATRIOT Act amendments to the Bank Secrecy Act, an additional checkbox "t" was added to the form for "Terrorist Financing."[149] Part IV of the form requires contact information for someone at the financial institution who may be able to provide further assistance to law enforcement, if necessary.[150]

Part V may be the most critical portion of the form.[151] It requires a lengthy free response, detailing the transaction and the reasons the financial institution may suspect illegal financial activity.[152] The financial institution must also describe any supporting documentation it has and all parties involved in the transaction.[153]

To assist financial institutions in reporting suspicious activity, FinCEN provides technical manuals and analytic reports to improve understanding of how money may be laundered in the future and how to identify it.[154] In addition, FinCEN issues regulations and interpretive guidance for financial institutions.[155] For example, FinCEN regularly publishes the SAR Activity Review, a periodical that provides "meaningful information about the preparation, use, and

147. *Id.*

148. The following is a comprehensive list of the checkboxes included on the form: Bank Secrecy Act/Structuring/Money Laundering, Bribery/Gratuity, Check Fraud, Check Kiting, Commercial Loan Fraud, Computer Intrusion, Consumer Loan Fraud, Counterfeit Check, Counterfeit Credit/Debit Card, Counterfeit Instrument (other), Credit Card Fraud, Debit Card Fraud, Defalcation/Embezzlement, False Statement, Misuse of Position or Self Dealing, Mortgage Loan Fraud, Mysterious Disappearance, Wire Transfer Fraud, Other (free response), Terrorist Financing, and Identity Theft. *Id.*

149. *See id.*; *see also* U.S. GOV'T ACCOUNTABILITY OFFICE, *supra* note 130, at 2 (discussing how the USA Patriot Act "expanded FinCEN's role to include a focus on terrorism financing as well as money laundering").

150. FINCEN, *supra* note 141.

151. *Id.* ("This section of the report is critical. The care with which it is written may make the difference in whether or not the described conduct and its possible criminal nature are clearly understood.").

152. *Id.*

153. See *id.* for a complete list of requirements for this free response question.

154. *See* U.S. GOV'T ACCOUNTABILITY OFFICE, *supra* note 130, at 9.

155. FFIEC, *supra* note 82, at 9.

value of Suspicious Activity Reports (SARs) filed by financial institutions."[156] Financial institutions rely upon FinCEN's findings and advice in identifying suspicious activity and when designing their detection algorithms used in their AML programs.[157]

III. RECOMMENDATION: IMPLEMENT A FOREIGN INTELLIGENCE DETECTION PROGRAM THAT BUILDS UPON THE CURRENT ANTI-MONEY LAUNDERING REQUIREMENTS

In response to growing concerns over terrorism finance, the USA PATRIOT Act expanded the scope of the AML requirements on financial institutions within the United States.[158] It provided the Secretary of the Treasury with the authority to impose on financial institutions requirements to store records and file suspicious activity reports when doing so would be useful for counterintelligence activities related to counterterrorism efforts.[159] This Article recommends that the scope of this requirement be expanded to encompass all U.S. counterintelligence activity, building off of the U.S. AML regime in a similar manner. Supporting this proposition, commentators have argued the efficacy of managing foreign intelligence threats similarly to those threats posed by international terrorism, including financial analysis.[160] Detailed in this section are the workflows that should be implemented to coordinate this new counterintelligence program, suggestions for promoting compliance by financial institutions, and possible typologies for identifying foreign intelligence activity.

156. FIN. CRIMES ENFORCEMENT NETWORK (FINCEN), SAR ACTIVITY REVIEW—TRENDS, TIPS & ISSUES, http://www.fincen.gov/news_room/rp/sar_tti.html (last visited Jan. 16, 2013).

157. *See, e.g.*, Cheng-wei Zhang & Yu-bo Wang, *Research on Application of Distributed Data Mining in Anti-Money Laundering Monitoring System*, 2D INT'L CONF. ON ADVANCED COMPUTER CONTROL 133 (2010) ("Some developed countries have constituted a set of electronic system[s] to detect money-laundering by the use of Expert System and Artificial Intelligence. For example, the FinCen in America built the FAIS . . . .").

158. U.S. GOV'T ACCOUNTABILITY OFFICE, *supra* note 130, at 7.

159. *Id.*

160. *See* Van Cleave, *supra* note 4, at 5 ("There is a parallel for thinking about counterintelligence as a strategic mission. Just as [U.S.] intelligence is mapping the essential features and activities of terrorist groups, so [counterintelligence] analysts could determine how foreign intelligence services are built and operate—call it [counterintelligence] order-of-battle preparation.").

A. Require Financial Institutions to File Suspicious Activity Reports for Suspected Foreign Intelligence Financial Transactions

The recommended workflow for the proposed counterintelligence program follows the practices and procedures already implemented in the current U.S. AML regime. Financial institutions would be required to make changes to their AML detection programs so that they could identify suspicious transactions that suggest possible foreign intelligence activity. Part III.C of this Article discusses recommendations for identifying these transactions. Upon discovering such a transaction, the financial institution would be required to retain documentation of the transaction and conduct an investigation into the transaction and the related clients, if possible. Following this investigation, the financial institution would be required to file a SAR with FinCEN noting its findings. The SAR form currently in use would remain substantially the same, with one modification: an additional checkbox labeled "Foreign Intelligence" would be added. The financial institution would check this box, and describe why it believes the transaction suggests foreign intelligence activity within the free response box in Part V of the SAR form.

Given the unwieldy volume of SARs already submitted to FinCEN and its inadequate resources to review all such reports,[161] review authority should fall to agencies already tasked with counterintelligence responsibilities. Foreign intelligence SARs filed with FinCEN would be forwarded to a new counterintelligence SAR review team.[162] Representatives from counterintelligence agencies responsible for domestic operations, such as the FBI, CIA and DIA, would comprise the team. However, the FBI should be responsible for leading the review team in light of its dominant role in domestic counterintelligence activity.[163]

161. *See* FATF, *supra* note 18, at 3.

162. This approach would mimic the SAR review teams recommended in the U.S. Department of Treasury's National Money Laundering Strategy, and the review teams currently implemented by the U.S. Internal Revenue Service. *See* U.S. GEN. ACCOUNTING OFFICE, GAO-03-813, COMBATING MONEY LAUNDERING: OPPORTUNITIES EXIST TO IMPROVE THE NATIONAL STRATEGY 26 (2003), *available at* http://www.gao.gov/new.items/d03813.pdf.

163. Furthermore, the FBI is responsible for the investigation of money

Further investigation would be at the discretion of the review team in light of the surrounding circumstances. For example, the review team may decide to forward the case to the FBI for investigation and possible prosecution. Or, the review team may decide that it would be more appropriate to engage in offensive counterintelligence measures through another agency, such as turning the identified individual into a double agent or providing the individual with misinformation intended to deceive the foreign intelligence service.[164] FinCEN already provides direct access to its SAR databases to law enforcement agencies,[165] meaning the review team could easily access the data. If a counterintelligence checkbox is added to the SAR form, this discrete piece of data could be used to distinguish those SARs in the FinCEN database. Furthermore, FinCEN could even limit the review team's access to those SARs related to counterintelligence, if that is preferred.

B. Promoting Compliance by the Financial Institutions

Disincentives exist for financial institutions to comply with these new requirements. Under the AML regime, financial institutions are responsible for financing the preventive measures such as the one proposed in this Article.[166] To pay for these programs, financial institutions usually must increase fees charged to clients, reduce overall profits, or do both.[167] However, compliance can be achieved by emphasizing those benefits that the financial institutions will derive through cooperation, as well as through designing the program to include additional economic incentives for those institutions that properly report counterintelligence

laundering related to crimes over which it has jurisdiction. FATF, *supra* note 18, at 4.

164. *See, e.g.*, Walter Pincus, *New Unit of DIA Will Take the Offensive on Counterintelligence*, WASH. POST, Aug. 18 2008, *available at* http://www.washingtonpost.com/wpdyn/content/article/2008/08/17/AR2008081702244.html ("The purpose of an offensive counterintelligence operation is not criminal prosecution . . . . In strategic offensive counterintelligence operations, a foreign intelligence officer is the target, and the main goals most often are 'to gather information, to make something happen. . . to thwart what the opposition is trying to do to us and to learn more about what they're trying to get from us.'" (quoting Toby Sullivan, Director of Counterintelligence)).

165. FATF, *supra* note 18, at 3.

166. Gordon, *supra* note 21, at 727.

167. *Id.*

SARs.

The first argument for cooperation by financial institutions is that it will assist the bank in providing prudential security. Prudential rules "are designed primarily to protect the safety and soundness of individual financial institutions and the financial system as a whole."[168] Financial institutions implement these rules to prevent the consequences stemming from risk related to significant loan defaults, or "putting all investment (typically lending) eggs in one financial basket."[169] Those foreign intelligence operations that are uncovered often lead to asset confiscation by the government.[170] Because illegals are increasingly using businesses in the United States under nonofficial cover, a financial institution that fails to comply with this new counterintelligence reporting regime may suffer financial setbacks if a discovered foreign intelligence cover business represents a significant portion of the institution's customer base.[171]

Financial institutions may ask: if the assets seized are to be confiscated, why would the institution have an incentive to turn in one of its clients? Under this new counterintelligence program, disincentives could be overcome by offering the financial institution a portion of the confiscated assets. More specifically, where banks submit a SAR detailing the possibility of foreign intelligence activity, the government could compensate banks with these assets. Where a foreign intelligence operation is discovered by law enforcement, however, and the financial institution failed to file a SAR when there was activity that should have raised suspicion or the institution failed to implement an adequate foreign intelligence detection system, the government would not

168. *Id.* at 706.

169. *Id.*

170. *See* Press Release, Fed. Bureau of Investigation, U.S. Dep't of Justice, Ten Russian Agents Plead Guilty and are to be Removed from the United States (Jul. 8, 2010), *available at* http://www.fbi.gov/newyork/press-releases/2010/nyfo070810a.htm ("[T]he defendants were required to disclose their true identities in court today and to forfeit certain assets attributable to the criminal offenses.").

171. This is known as concentration risk. See DIANE REYNOLDS, ANALYZING CONCENTRATION RISK (2009), *available at* http://www.algorithmics.com/EN/media/pdfs/Algo-WP0109AnalyzingConRisk.pdf for a detailed explanation of calculating concentration and credit risk.

compensate the institution from the seized assets. Thus, the financial institution will have economic incentives to implement this proposal effectively within their AML program; if they do not, they will lose out on this compensation.

To sweeten the pot, the FBI could offer a cash reward to any financial institution that discovers a foreign intelligence operation and files a SAR accordingly. The FBI currently offers rewards to anyone who provides information leading to the arrest and conviction of a spy.[172] Indeed, the FBI will pay up to $500,000 for this information.[173] This sizeable reward may provide an additional incentive for financial institutions to comply with the new requirements.

Without doubt, there will be some financial institutions that will find these incentives insufficient to justify the costs of implementing the new counterintelligence detection and reporting requirements. All financial institutions would be required to follow the new requirements, but there is no guarantee that any one particular financial institution will find a spy among its clients. Thus, regulatory risk must also be imposed. The current AML regime already imposes stiff regulatory burdens on those financial institutions that fail to comply with AML requirements.[174] A bank that fails to comply would risk severe monetary penalties and the possibility of seeing its bank charter revoked.[175] Furthermore, those bank employees involved in the violation risk being removed from the financial institution and barred from banking.[176] Similar penalties could be imposed upon banks and other financial institutions that fail to comply with the newly imposed counterintelligence program requirements. Compliance testing can be conducted in conjunction with general AML examination testing

172. Fed. Bureau of Investigation, *Counterintelligence*, http://www.fbi.gov/about-us/investigate/counterintelligence/counterintelligence (last visited Jan. 16, 2013) ("Report Espionage! You can pocket up to $500,000 for information that leads to the arrest and conviction of a spy or to the prevention of espionage. To report suspicious activities, contact your local field office or submit an anonymous tip.").

173. *Id.*

174. *See* FFIEC, *supra* note 82, at 14 (explaining the criminal and civil penalties for financial institutions that fail to comply with AML requirements).

175. *Id.*

176. *Id.*

procedures already conducted by the Federal Financial Institutions Examination Council.[177]

C. Financial Transaction Typologies That May Suggest Foreign Intelligence Activity

Of course, requiring financial institutions to report this information would be useless unless these institutions were provided foreign intelligence typologies. Providing financial institutions with the knowledge of what a foreign intelligence transaction would look like would be the key to the success of this counterintelligence program. Illustrating this point, many commentators have noted that one of the major weaknesses of the current counterterrorism finance regime is that financial institutions are not offered adequate information on the typologies that suggest terrorism finance.[178] Furthermore, feedback regarding the helpfulness of the information is rarely provided to financial institutions that file SARs.[179]

Thus, the agencies responsible for the counterintelligence program using the AML regime as a tool for uncovering foreign intelligence threats must provide financial institutions with possible typologies. FinCEN could fund an analytic review of all SARs filed for all illegals and American spies caught since FinCEN's inception. If typologies do emerge, they could provide this information to financial institutions and tailor the requirements to account for any compliance burden that may arise. In addition, interested counterintelligence units from organizations such as FBI, CIA, DIA, and NCIX, among others, could collaborate to propose some suggested typologies based upon their collective experience of uncovering spies.

While developing a comprehensive list of typologies for detecting foreign intelligence activities within the United States would be outside the scope of this Article, this section

177. See *id.* for a detailed description of current AML examination techniques.

178. *See* U.S. GOV'T ACCOUNTABILITY OFFICE, *supra* note 130, at 27 ("In this report, we recommended that FinCEN further develop and document its strategy to fully incorporate best practices to help enhance and sustain collaboration among federal agencies in the form change process and distribute that documentation to all stakeholders."); Gordon, *supra* note 21, at 727.

179. *Id.*

will discuss those client or transaction characteristics that could most readily be included in such a list.

1. Client is Employed in an Industry Frequently Targeted by Foreign Intelligence Agencies

The primary indicator that a transaction is related to foreign intelligence activity would be a suspicious transaction conducted by an individual employed by the federal government or in an industry frequently targeted by foreign intelligence agencies. In a study conducted by the Defense Personnel Security Research Center (PERSEREC), the Center found money to be the dominant factor that led Americans to spy on their own country.[180] While nearly half of those Americans engaged in espionage were never paid, this is primarily because counterintelligence officers caught most perpetrators before they could transmit information.[181]

Aldrich Ames, one of the most famous American spies who passed information to the Soviets over the course of a decade, reportedly received nearly three million dollars.[182] During this time, Ames purchased an expensive home and automobile in cash.[183] It is unlikely that he could have afforded this behavior on the meager CIA salary he was receiving at the time.[184] While Ames's conspicuous antics would probably alert counterintelligence security personnel regardless of any AML monitoring component, AML efforts would be able to detect similar but less extreme cases of espionage in the future. Suspicious transactions made by employees frequently targeted by foreign intelligence services could prompt the financial institution to check the Foreign Intelligence box on the SAR form.

To aid in this effort, these employees should receive heightened scrutiny under the AML due diligence requirements. Such efforts could mimic the heightened due diligence requirements already imposed on PEPs, where

180. HERBIG & WISKOFF, *supra* note 33, at xii. PERSEREC maintains a database of information on those individuals known to have engaged in espionage against the United States, and provides analytic reports summarizing the data and suggesting common characteristics that have motivated spies in the past. *Id.* at v.

181. *Id.* at xi.

182. TURNER, *supra* note 24, at 134.

183. *Id.* at 136.

184. *Id.*

financial institutions give greater review to those customers who are considered to be more risky. When ascertaining the identity and occupation of the client, the bank could make an effort to identify the client's employer. Those clients working for the government, within the defense industry, and in industries involved in sensitive technologies would receive greater AML scrutiny. Similar measures should also be taken for those clients working for a government contractor or companies similarly associated with U.S. policymakers. Indeed, one-fourth of civilian American spies worked for contractors at the time they engaged in acts of espionage.[185]

Because financial institutions will absorb the majority of these heightened monitoring costs, the counterintelligence community should take on the responsibility of identifying the industries and corporations that are most at-risk and therefore deserve increased attention. It would be the counterintelligence community that has the most readily available information on employers that are at-risk of foreign intelligence penetration. Outside of the defense and weapons industries, the technologies most heavily targeted by foreign intelligence collectors include "aeronautics, information systems, lasers and optics, sensors, and marine systems."[186] Counterintelligence officials could compile lists of companies within these industries, as well as those government agencies and contractors that warrant increased scrutiny. Such a process would need to be continuous, as government organization and economic situations change over time.

2. Client Has Poor Credit

Credit ratings could also be used by financial institutions to identify espionage. Of those Americans who committed espionage on behalf of other countries for money, only about twenty percent committed espionage for purposes of greed.[187] In contrast, half of these Americans engaged in espionage

185. HERBIG & WISKOFF, *supra* note 33, at xi.

186. ONCIX, *supra* note 8, at iii.

187. HERBIG & WISKOFF, *supra* note 33, at 41. "Some people spied for money because they needed it to pay off debts or to get themselves out of some other fix, while others did so from greed. We coded 'need or greed' variables and the type of financial pressures or luxury purchases reported for our cases where these details were available." *Id.* at 40.

because they were in financial trouble.[188] This can include financial insolvency, bankruptcy, or late payments on various forms of debt.[189] For example, Russian KGB operatives recruited Richard Miller, an FBI counterintelligence officer struggling to make his mortgage payments.[190] He traded classified material for $50,000 in gold, several cash payments of unknown amounts, and sexual favors from a female KGB officer.[191] Similarly, Bruce Ott of the U.S. Air Force attempted to pass classified material to the KGB in 1986 to alleviate his debt problems.[192] Ott's peer described him as "'a spendthrift who bounced checks, overused his credit cards, had his car repossessed, and was in such financial trouble on his honeymoon that his wife footed the entire bill.'"[193] While this Article has already proposed imposing heightened due diligence on all employees within the government and sensitive technology industries, poor credit ratings of those employees could warrant the highest form of scrutiny.

In the alternative, credit ratings could be used as a means of limiting the number of employees subject to heightened scrutiny. For example, if financial institutions argue that it would be economically unfeasible to impose increased due diligence standards on all employees within the government and sensitive technology industries, credit ratings could be used to narrow the scope of the scrutiny to those employees most at-risk of espionage recruitment.

3. The Transaction Involves a Possible Foreign Intelligence Front Organization

Foreign intelligence services engage extensively in covert intelligence operations within the United States using "front organizations."[194] The goals of these organizations are to conduct business that advances the intelligence service's interests without maintaining any apparent links to a foreign government, or provide nonofficial cover for intelligence

188. *Id.*
189. *Id.*
190. *Id.*
191. *Id.* at 40–41.
192. *Id.* at 41.
193. *Id.* (quoting G. Kell, *Alleged Spy "Glad It Was Over*," SACRAMENTO BEE, July 31, 1986).
194. Kevin A. O'Brien, *Covert Action: The "Quiet Option" in International Statecraft*, *in* 3 STRATEGIC INTELLIGENCE 23, 40 (Loch K. Johnson ed., 2007).

operatives.[195] Identification of money laundering activities conducted by these front organizations could prompt a financial institution to file a foreign intelligence SAR.

This Article recognizes three instances where financial institutions should file a foreign intelligence SAR when an organization or company within the United States engages in suspicious financial activity. First, some front organizations do indeed have overt ties to a foreign nation's government.[196] For example, communist and socialist parties have engaged in political advocacy in the past through the use of front organizations.[197] Other organizations are owned and controlled directly by another nation's government and there are some intelligence services that take advantage of this control.[198] For example, during the Cold War, the KGB would often act as a filter for any Soviet organization operating in a foreign country.[199] Any suspicious transactions carried out by such organizations should be reported through a foreign intelligence SAR.

Second, an organization or company that attempts to hide the nature of its control may justify the filing of a foreign intelligence SAR. A shell company is an entity such as a corporation, limited liability company, or trust that has no physical presence except a mailing address and generates little, if any, economic value.[200] Shell companies use "bearer shares, nominee shareholders, and nominee directors . . . to mask ownership in [the] corporate entity."[201] The AML community has already identified the use of shell companies in transactions as a potential indicator of general money laundering activity.[202] While shell companies are often used

195. *See id.*
196. *See id.*
197. *See id.*
198. *See id.*
199. *Id.*
200. *See* U.S. MONEY LAUNDERING THREAT ASSESSMENT WORKING GRP., U.S. MONEY LAUNDERING THREAT ASSESSMENT 47 (2005), *available at* http://www.ffiec.gov/bsa_aml_infobase/documents/new_6_2006/FinCEN%20Feb%2006%20ML.pdf.
201. *Id.*
202. *See* FIN. CRIMES ENFORCEMENT NETWORK (FINCEN), FIN-2006-G014, POTENTIAL MONEY LAUNDERING RISKS RELATED TO SHELL COMPANIES (2006), *passim*, *available at* http://www.fincen.gov/statutes_regs/guidance/pdf/AdvisoryOnShells_FINAL.pdf ("Shell companies have become common tools for money laundering and other financial crimes, primarily because they are easy and

for legitimate purposes, they can be used in illicit transactions to hide the true identities of the company owners.[203]

Some front organizations begin as a legitimate enterprise but their control is later assumed by foreign intelligence services.[204] If a company doing business in the United States were to engage in transactions with a shell company, the financial institution may investigate the nature of the transaction. If it becomes apparent that the shell company is being used to hide the origin of control, and if that control is connected to a foreign nation, this type of transaction may suggest foreign intelligence operations and may warrant a filing.

Third, regardless of their ownership or origin, organizations and companies doing business in the sensitive technology industries should also be subject to a level of heightened scrutiny, similar to the previously suggested scrutiny imposed upon individuals employed within that industry. Foreign intelligence SAR filings would be appropriate for any suspicious transaction conducted by a company in one of these industries.

CONCLUSION

The United States currently has an intricate system in place to monitor financial transactions for irregular activity that may suggest criminal behavior. At the present time, the system is designed to defeat money laundering and terrorism finance efforts. With several small changes, however, the system could be used as a powerful tool in the detection of foreign intelligence activity. A counterintelligence program that uses the current AML regime would not be foolproof; many spies have motivations beyond monetary gain.[205] But the transactions of those individuals and organizations that are increasingly targeted by foreign intelligence services would be under much greater scrutiny and could provide

inexpensive to form and operate.").

203. U.S. MONEY LAUNDERING THREAT ASSESSMENT WORKING GRP., *supra* note 200, at 47–48 ("The use of these legal structures for money laundering is well established."); *see* FINCEN, *supra* note 202, at 4.

204. *See* U.S. MONEY LAUNDERING THREAT ASSESSMENT WORKING GRP., *supra* note 200, at 47.

205. *See* HERBIG & WISKOFF, *supra* note 33, at 40.

counterintelligence officials a wealth of information about potential threats.

The advantages of implementing such a system are apparent. First, many SARs filed by financial institutions are not sufficiently scrutinized for counterintelligence-related activity by FinCEN because of the agency's decision to prioritize terrorism finance-related transactions. The proposed program would use counterintelligence resources to analyze many of the unviewed SARs, which could improve counterintelligence operations. Second, the program would improve detection of suspicious transactions related to foreign intelligence by prompting a concerted effort by counterintelligence officials to suggest and provide financial institutions with concrete typologies of such transactions. And third, it would make those employees and organizations in a position to be targeted by foreign intelligence services under heightened scrutiny in the current AML regime.

Ultimately, it is important to remember that AML efforts are not unique to the United States.[206] Nothing prevents foreign nations from conducting similar counterintelligence operations using their own AML programs. One thing is certain: lessons that may be learned from the implementation of this program would provide our own U.S. intelligence officers working overseas the know-how and capabilities of concealing their transactions and avoiding detection by foreign counterintelligence units. Should the United States fall behind in the cat-and-mouse world of intelligence? Or should it remain one step ahead of its adversaries, pioneering a new form of proactive counterintelligence?

206. Most AML laws implemented by the United States are in accordance with international standards set forth by FATF. SCHOTT, *supra* note 22, at III-7–III-8.