JEB HENSARLING, TX , CHAIRMAN

United States House of Representatives
Committee on Financial Services
2129 Rayburn House Office Building
Washington, D.C. 20515

MAXINE WATERS, CA, RANKING MEMBER

MEMORANDUM

To: Members of the Committee on Financial Services

From: FSC Majority and Minority Staff

Date: June 22, 2015

Subject: June 24, 2015, Task Force to Investigate Terrorism Financing hearing titled "Evaluating the Security of the U.S. Financial Sector"

The Task Force to Investigate Terrorism Financing will hold a hearing entitled "Evaluating the Security of the U.S. Financial Sector" on Wednesday, June 24, 2015, at 2:00 p.m. in room 2128 of the Rayburn House Office Building. This will be a one-panel hearing with the following witnesses:

- The Honorable Cyrus Vance, Jr., District Attorney, New York County District Attorney's Office
- Mr. Chip Poncy, Founding Partner, Financial Integrity Network; Senior Counselor, Center on Sanctions and Illicit Finance at the Foundation for Defense of Democracies
- Mr. John W. Carlson, Chief of Staff, Financial Services Information Sharing and Analysis Center

Introduction

Terrorist groups and actors are constantly seeking to exploit the U.S. financial system to fund their operations and launder their revenue. The growth and complexity of the international financial system has also enabled illicit actors to place and move money, hide assets, and conduct transactions anywhere in the world, exposing financial centers to exploitation and abuse. These actors seek to circumvent anti-money laundering and counter-terrorist financing measures by, among other things, taking advantage of the unsettled area of beneficial ownership to form shell corporations. Moreover, the U.S. has seen terrorist groups use banks to place and transfer funds, along with cash transportation provided by cash couriers.

The U.S. financial services sector has also been recognized as a prime target for sophisticated and organized cyber attacks. The increase in the frequency and breadth of attacks on banks can be attributed to banks holding not only money but also sensitive personally identifiable information and clients' intellectual property. In light of this trend, the financial sector is considered to be one of the most experienced industries at dealing with cyber attacks.

Beneficial Ownership

Background

Terrorists and criminals have created and used shell companies to both disguise and finance their activities.[1] Shell companies are business entities whose ambiguous or deceptive ownership structures hide the identities of the people who ultimately control or profit from the companies – the "beneficial owners."[2] Such untraceable shell companies have few, if any, employees and can be used to hide illegal businesses or facilitate illegal activity, such as tax evasion and Ponzi schemes that can rob billions from unsuspecting citizens.[3] They have been described as "the vehicle of choice for money launderers, bribe givers and takers, sanctions busters, tax evaders and financers of terrorism,"[4] because they are an ideal mechanism for international money launderers since information on their beneficial owners is often unavailable to law enforcement.[5] Currently, there is no process

[1] Diana L. Ohlbaum, "Terrorism, Inc. How Shell Companies Aid Terrorism, Crime and Corruption," *Open Society Foundations* (October 2013), *available at* http://www.opensocietyfoundations.org/briefing-papers/terrorism-inc-how-shell-companies-aid-terrorism-crime-and-corruption.
[2] *Id.*
[3] *Id.*
[4] *See* "Launderers Anonymous: A Study Highlights How Easy It Is to Set Up Untraceable Companies," *the Economist* (September 22, 2012), *available at http://www.economist.com/node/21563286.*
[5] U.S. Senate, Caucus on International Narcotics Control, *The Buck Stops Here: Improving U.S. Anti-Money Laundering Practices* (April 25, 2013), *available at* http://www.drugcaucus.senate.gov/sites/default/files/Money%20Laundering%20Report%20-%20Final.pdf; Leslie Wayne, "How Delaware Thrives as a Corporate Tax Haven," *The New York Times* (June 30, 2012), *available at* http://www.nytimes.com/2012/07/01/business/how-delaware-thrives-as-a-corporate-tax-haven.html?_r=0.

in place to keep an updated list of the names of the beneficial owners of corporations or limited liability companies (LLCs) formed pursuant to state laws.[6]

The U.S. is a preferred destination for illicit actors from around the world to set up companies for the purpose of moving or hiding dirty money.[7] For example, the son of Equatorial Guinea's dictator, Teodoro Obiang, purchased a $30 million mansion in Malibu and a jet using shell companies based in California and the British Virgin Islands;[8] Hezbollah financed its activities in part by using shell companies in North Carolina to smuggle cigarettes to finance terrorism;[9] and Russian arms trafficker Viktor Bout used at least a dozen shell companies in Delaware, Texas, and Florida to operate his global arms smuggling operation.[10] Shell companies have also been used to bribe Russian officials, defraud the E.U., and evade Iranian sanctions.[11]

The international community has also examined the misuse of corporate vehicles for illicit purposes. In particular, the FATF,[12] the World Bank, and the United Nations Office of Drugs and Crime Stolen Asset Recovery Initiative[13] have explored the misuse of corporate vehicles for illicit purposes. In general, these studies found the lack of sufficient, accurate and timely beneficial ownership information facilitated money laundering and terrorist financing by disguising: (1) the identity of known or suspected criminals, (2) the true purpose of an account or property held by a corporate vehicle, and (3) the source or use of funds or property associated with a corporate vehicle.[14]

Congressional Action on Beneficial Ownership

Since May 2008, Congress has addressed the issue of beneficial ownership through bipartisan legislation known as the "Incorporation Transparency and Law Enforcement Act." This bill would have required the disclosure of beneficial owners at the time of incorporation, and would have made such information available to only law enforcement. A version of this bipartisan bill has been introduced in every successive session of Congress through 2013. The latest Senate version of the bill[15] would require states to add a single

---

[6] *Id.*
[7] *See* World Bank and UNODC Stolen Asset Recovery Initiative, *The Puppet Masters,* World Bank (2011).
[8] Anonymous Companies: How Hidden Company Ownership is a Major Barrier in the Fight Against Poverty and What to Do About It, Global Witness (December 2013), *available at* *file:///F:/Terrorist%20Financing/Hearing%20%233/Anonymous%20Companies%20Global%20Witness%20briefing.pdf*.
[9] Dennis M. Lormel, "It's Time to Pry Criminals Out of Their Shell (Companies)," *Cleveland Plain Dealer* (August 16, 2013, *available at* http://www.cleveland.com/opinion/index.ssf/2013/08/its_time_to_pry_criminals_out.html.
[10] *Id.*
[11] *See* Anonymous Companies, *supra*, note 10.
[12] FATF (2206) and FATF & CFATF (2010).
[13] *See* World Bank and UNODC Stolen Asset Recovery Initiative, *supra*, note 7.
[14] *See* Financial Action Task Force Report, *Transparency and Beneficial Ownership*, October 2014, *available at* http://www.fatf-gafi.org/media/fatf/documents/reports/Guidance-transparency-beneficial-ownership.pdf.
[15] *See* Statement of Senator Carl Levin (D-Mich), On Introduction of the Incorporation and Law Enforcement Assistant Act (August 1, 2013).

additional question to their existing incorporation forms to provide the names of the beneficial owners of corporations being formed.[16] The National Association of Secretaries of State has opposed this legislation due to concerns over implementation costs.[17]

The Administration's Beneficial Ownership Action Plan

In June 2013, the G8 in Lough Erne, Northern Ireland met and agreed to an action plan to prevent the misuse of shell companies and similar legal arrangements. The action plan required companies to maintain their beneficial ownership information and that the information should be available to law enforcement and other competent authorities.[18] Additionally, countries were to consider making such information available to financial institutions and other regulated businesses.[19] Trust information should be collected and available, the principles explained, but only to law enforcement.[20] These principles were largely reiterated by the Financial Action Task Force (FATF)—the body setting international anti-money laundering standards—in their Guidance on Transparency and Beneficial Ownership in October 2014 and by the G20 in their High Level Principles on Beneficial Ownership in November 2014.[21]

On June 18, 2013, the Administration announced the "National Action Plan on Preventing the Misuse of Companies and Legal Arrangements" where it defined beneficial ownership as a "natural person who, directly or indirectly, exercises substantial control over a covered legal entity or has a substantial economic interest in, or receives substantial economic benefit from, such legal entity, subject to several exceptions." [22] The plan would also ensure law enforcement authorities, including tax authorities, would be able to access beneficial ownership information upon appropriate request through a central registry at the state level.[23]

In March 2014, the Administration announced a legislative proposal intended to help law enforcement investigate the use of shell companies established solely for illegal activity.[24] The proposal would require all companies formed in any state to obtain a

---

[16] Incorporation Transparency and Law Enforcement Act, S. 1465, 113th Cong. (2013).
[17] *See* National Association of Secretaries of State, *NASS Company Formation Task Force*, http://www.nass.org/nass-initiatives/nass-company-formation-task-force/
[18] Liz Confalone, "A Brief, Recent History of Beneficial Ownership Transparency on the Global Agenda," *Global Financial Integrity* (December 5, 2014), *available at* http://www.gfintegrity.org/brief-recent-history-beneficial-ownership-transparency-global-agenda/.
[19] *Id.*
[20] *Id.*
[21] *Id.*
[22] *See* The White House Office of the Press Secretary, *United States G-8 Action Plan for Transparency of Company Ownership and Control* (June 18, 2013), *available at* https://www.whitehouse.gov/the-press-office/2013/06/18/united-states-g-8-action-plan-transparency-company-ownership-and-control.

[23] *Id.*
[24] The White House Blog, Beneficial Ownership Legislation Proposal (April, 4, 2014), *available at* https://www.whitehouse.gov/blog/2014/04/04/beneficial-ownership-legislation-proposal.

federal tax employee identification number.[25] This would be achieved by requiring the IRS to collect the beneficial owner information of all legal entities organized in any state.[26] The IRS would also be allowed to share this information with law enforcement officials to identify and investigate persons who form and misuse U.S. corporate structures to launder criminal proceeds and finance terrorism through the banking system.[27] The proposal has not received congressional sponsorship.

Actions by the Treasury Department

The Treasury's Financial Crimes Enforcement Network (FinCEN) issued an Advance Notice of Proposed Rulemaking on customer due diligence by financial institutions in March 2012. On July 30, 2014, FinCEN issued a Notice of Proposed Rulemaking (NPRM) that added a new element requiring financial institutions to know and verify the identities of the beneficial owners, or the real people who own, control and profit from the companies planning to use their services.[28] This rule was intended to increase financial transparency and further the U.S.'s commitment in the G-8 Action Plan for Transparency of Company Ownership and Control.[29] Under the proposed rule, a financial institution would require any person opening an account to fill out a form identifying themself, the legal entity for which the person is opening the account, and any beneficial owners associated with the legal entity.[30] The proposal defines "beneficial owner" as any individual who owns 25% or more of the equity interest in the legal entity, or an individual with "significant responsibility" to control the entity.[31] The person opening the account would furnish on the form a beneficial owner's name, address, date of birth and social security (or passport) number.[32] Concerns about these proposals have been raised by groups such as the American Bankers Association and the Bankers Association for Finance and Trade. In particular, these groups have argued that the proposals would impose an undue burden and expense on banks.[33] FinCEN has received and is currently reviewing approximately 130 comments on the NPRM.

---

[25] *Id.*
[26] *Id.*
[27] *Id.*
[28] *See* Samuel Rubenfeld, *Proposed Rule to Force Banks to Identify Beneficial Owners*, *The Wall Street Journal* (July 30, 2014), *available at* http://blogs.wsj.com/riskandcompliance/2014/07/30/u-s-treasury-proposes-rule-forcing-banks-to-identify-beneficial-owners/.
[29] The U.S. Treasury Press Center, *Treasury Issues Proposed Rules to Enhance Financial Transparency* (July 30, 2014), *available at* http://www.treasury.gov/press-center/press-releases/Pages/jl2595.aspx.
[30] *Id.*
[31] *Id.*
[32] *Id.*
[33] Mary Beth Goodman, "Beneficial Ownership Rules Would Drag Criminals into Daylight," *American Banker* (February 18, 2015), *available at* http://www.americanbanker.com/bankthink/beneficial-ownership-rules-would-drag-criminals-into-daylight-1072763-1.html.

Moving and Placing Funds: Vulnerabilities and Risks[34]

The growth and increasing sophistication of the international financial system in recent years has enabled illicit actors to place and move money, hide assets, and conduct transactions anywhere in the world, exposing financial centers to exploitation and abuse in an unprecedented way. The United States has seen a wide variety of terrorist groups, including al Qaeda (AQ) and its affiliates, Al-Shabaab, Hamas and Hizballah, use banks[35] to place and transfer funds, along with cash transportation provided by cash couriers.

The AML/CFT controls required by the U.S. regulatory framework aid financial institutions in identifying risk, provide valuable information to law enforcement, and inform U.S. national security policy. These required measures include the establishment of AML programs and reporting and record keeping requirements to provide useful information to law enforcement and national security authorities for the purpose of combating the full range of illicit finance threats. An AML program must include, at a minimum, a system of internal controls to ensure ongoing compliance, independent testing, designation of an individual responsible for managing BSA compliance and training for appropriate personnel.[36] An effective AML/CFT regime also includes enhanced due diligence procedures for those customers that present a high risk for money laundering or terrorist financing (TF), as well as for the provision of foreign correspondent accounts and private banking services.[37] However, when these safeguards are not effectively implemented or stringently enforced, money launderers, terrorist financiers and other illicit actors are able to abuse the U.S. financial system.

The combination of a strong AML/CFT legal framework and effective supervision has succeeded in making it more difficult for terrorists and their facilitators to access the U.S. financial system, often forcing support networks to resort to costlier and/or riskier means of meeting their operational needs.[38]

---

[34] The section entitled "Moving and Placing Funds: Vulnerabilities and Risks" is derived nearly verbatim from the U.S. Department of the Treasury, *National Terrorist Financing Risk Assessment*, (June 2015), *available* at http://www.treasury.gov/resource-center/terrorist-illicit-finance/Documents/National%20Terrorist%20Financing%20Risk%20Assessment%20%E2%80%93%2006-12-2015.pdf.

[35] Under the BSA, as implemented by 31 C.F.R. § 1010.100, the term "bank" includes each agent, agency, branch or office within the U.S. of commercial banks, savings and loan associations, thrift institutions, credit unions, and foreign banks. The term "bank" is used throughout this document generically to refer to these financial institutions.

[36] *See, e.g.,* 12 C.F.R. § 21.21 (national banks); 12 C.F.R. § 208.61 (state member banks); 12 C.F.R. § 326.8 (nonmember banks); 12 C.F.R. § 748.2 (credit unions); FINRA Rule 3310 (securities broker-dealers); and National Futures Association Rule 2-9(c) (commodities brokers and futures commission merchants). *See also* Federal Financial Institutions Examination Council (FFIEC) BSA/AML Examination Manual (2014), pp. 28-29. Available at https://www.ffiec.gov/bsa_aml_infobase/documents/BSA_AML_Man_2014.pdf.

[37] *See id*. at 112-118 & 125-129. *See also* Joint Guidance on Obtaining and Retaining Beneficial Ownership Information, FIN– 2010–G001, March 5, 2010.

[38] *See* David Cohen, Under Secretary for Terrorism and Financial Intelligence, Department of the Treasury, Remarks before the Center for a New American Security, "Confronting New Threats in Terrorist Financing,'" March 4, 2014.

Broadly speaking, based on an analysis of U.S. law enforcement investigations and prosecutions relating to TF, two methods of moving money to terrorists and terrorist organizations have been predominate in the convictions and cases pending since 2001: the physical movement of cash and the movement of funds through the banking system.[39] Funds moved through the banking system were placed into the banking system by directly depositing cash at a bank. The physical movement of cash accounted for 28 percent of these cases while movement directly through banks constituted 22 percent.

Banks

Banks are an attractive means for terrorist groups seeking to move funds globally because of the speed and ease at which they can move funds within the international financial system.[40] Through their global networks and inter-bank relationships, U.S. banks can instantly transfer funds for their customers almost anywhere in the world. Additionally, because of the importance of the United States to global financial markets activity, many foreign banks have established subsidiary branches or agencies in the United States to gain access to U.S.-based customers and to serve their own local customers' needs in the United States.

In light of this vulnerability, the U.S. government has implemented an AML/CFT regulatory framework that includes robust implementation of targeted financial sanctions, which has made it more difficult for terrorists and their support networks to access the U.S. financial system. This framework aids financial institutions in identifying and managing risk, provides valuable information to law enforcement, and creates the foundation of financial transparency required to apply targeted financial measures against the various national security threats that seek to operate within the U.S. financial system.[41]

OFAC administers and enforces a vigorous sanctions regime in collaboration with the regulatory, law enforcement, and intelligence communities. Violators of U.S. economic sanctions can be subject to a range of administrative, civil and criminal penalties. The federal banking agencies[42] conduct regular examinations of banks to ensure compliance with BSA/AML programs, including ensuring that such institutions have an effective

[39] An analysis was conducted by Treasury on terrorism and terrorism-related convictions between 2001 and 2014. Using publicly available documents (indictments, sentencing memoranda, law enforcement press releases, media reports, etc.) the cases were examined more closely in order to determine key financial components. In the 229 cases surveyed, 96 included information on the financial component to the investigation, either raising or moving the funds. These cases were then further analyzed to determine what specific method or channel was used to raise or move funds.

[40] *See* FATF, Terrorist Financing, p. 21, February 2008.

[41] David Cohen, Under Secretary for Terrorism and Financial Intelligence, Department of the Treasury, Testimony before the Senate Committee on Homeland Security and Governmental Affairs Permanent Subcommittee on Investigations, "U.S. Vulnerabilities to Money Laundering, Drugs, and Terrorist Financing: HSBC Case History," July 17, 2012. Available at http://www.hsgac.senate.gov/download/?id=55d94bbb-cbee-4a35-89ca-5493a12d73dd.

[42] For the purposes of the National TF Risk Assessment, the relevant federal banking agencies are the FRB, the FDIC, NCUA and OCC.

BSA/AML and OFAC compliance program that: identifies higher-risk areas, provides for appropriate internal controls for screening and reporting, establishes independent testing for compliance, designates an employee or employees as responsible for OFAC compliance, and creates training programs for appropriate personnel.[43] The SEC and CFTC impose similar requirements on financial institutions they supervise.

The enactment of the USA PATRIOT Act following the September 11, 2001 terrorist attacks enhanced the efforts of the U.S. government to prevent the U.S. financial system from being used to facilitate TF. For example, under Section 311 of the USA PATRIOT Act, the Secretary of the Treasury is authorized to find a foreign jurisdiction, foreign financial institution, class of international transactions, or type of account to be of primary money laundering concern, and to subsequently impose any one or a combination of special measures that U.S. financial institutions must take to protect the U.S. financial system, including from risks associated with TF.[44] These special measures range from enhanced due diligence, recordkeeping, and reporting requirements, up to and including, prohibition against establishing or maintaining any correspondent account or payable through account for or on behalf of a foreign financial institution, if the account involves a jurisdiction, financial institution, class of transaction, or type of account that is of primary money laundering concern. Treasury, through FinCEN, has utilized Section 311 to alert the U.S. financial system to TF threats associated with several foreign jurisdictions and foreign financial institutions, including: the Islamic Republic of Iran; LCB; the Commercial Bank of Syria (CBS) (including its subsidiary Syrian Lebanese Commercial Bank); Halawi Exchange Co.; and Kassem Rmeiti & Co.[45] In finding that CBS was a financial institution of primary money laundering concern, FinCEN noted that "numerous transactions that may be indicative of terrorist financing and money laundering have been observed transiting CBS," including "several transactions through accounts at CBS that reference a reputed financier for Osama bin Laden."[46]

In addition to Section 311, Sections 314(a) and 319 of the USA PATRIOT Act strengthened the U.S. government's ability to take specific regulatory actions to advance law enforcement investigations against TF threats. Section 314(a) allows law enforcement authorities to share information with financial institutions regarding individuals, entities, and organizations engaged in or reasonably suspected of engaging in terrorist acts and to determine whether the target of an investigation maintains an account at a particular financial institution.[47] Section 319(a) enhances law enforcement's ability to pursue assets overseas, while Section 319(b) provides law enforcement with summons and subpoena

[43] The Federal Financial Institutions Examination Council (FFIEC) BSA/AML Examination Manual includes specific portions on compliance with OFAC's targeted financial sanctions regime. See FFIEC BSA/AML Manual 2014, pp. 145-154.
[44] *See* 31 U.S.C. § 5318A.
[45] A list of Section 311 Special Measures taken by FinCEN is available at http://www.fincen.gov/statutes_regs/patriot/section311.html.
[46] FinCEN, Imposition of a Special Measure Against Commercial Bank of Syria, Including Its Subsidiary, Syrian Lebanese Commercial Bank, as a Financial Institution of Primary Money Laundering Concern, Notice of Proposed Rulemaking, 69 Fed. Reg. 28098, 28100, May 18, 2004.
[47] *See* 31 U.S.C. § 5318.

authority with respect to foreign banks that have correspondent accounts in the United States.[48]

Punitive measures and, for egregious cases, financial penalties, have been applied to banks determined to be out of compliance. For example, in December 2012, HSBC, a UK-headquartered financial institution with a substantial U.S. presence, was ordered to pay a total of approximately $1.9 billion in civil money penalties and asset forfeitures for various violations of U.S. AML and economic sanctions laws and regulations.[49] Furthermore, in a July 2014 settlement with U.S. regulators and law enforcement, BNP Paribas, in addition to having to pay a total of approximately $8.9 billion in criminal penalties and asset forfeitures, was subjected to a one-year long suspension of certain U.S. dollar-clearing services through its New York branch and other affiliates for business lines on which the misconduct centered.[50] FinCEN has also imposed civil money penalties against U.S. branches of foreign banks for failing to implement adequate due diligence procedures and internal controls that effectively managed the risk arising from the provision of foreign correspondent accounts or dollar-clearing services to financial institutions located in jurisdictions deemed a high-risk for money laundering and TF.[51]

Misuse of Foreign Correspondent Banking

The regulatory and enforcement actions taken by the U.S. government and the subsequent substantial financial and organizational investments by U.S.-based financial institutions have improved AML/CFT compliance among financial institutions.[52] However, the international financial system is interconnected and foreign financial institutions maintain correspondent accounts at and receive services from U.S. financial institutions in order to access the U.S. financial system. These relationships allow financial institutions worldwide to facilitate cross border transactions in the currency of choice. They also enable financial institutions to conduct business and provide services to clients in foreign countries without the expense and burden of establishing a foreign presence. However, some correspondent banking relationships are inherently higher-risk, in large part due to the challenges of "intermediation," where multiple intermediary financial institutions may be involved in a single funds transfer transaction. The complexity and volume of transactions that flow through U.S. correspondent accounts, coupled with the varying

[48] *See* 18 U.S.C. § 981(k); 31 U.S.C. § 5318(k)(3).
[49] *See* OCC EA 2012-261, AA-EC-2012-140, December 4, 2012 and FRB Docket Nos. 12-062-CMP-FB, 12-062-CMPHC,and 12-062-B-FB, 2-4, December 11, 2012; FinCEN, *In the Matter of HSBC Bank USA, N.A. Mclean, Virginia*, No. 2012-02, December 10, 2012; *see also* Senate Permanent Subcommittee on Investigations, U.S. Vulnerabilities to Money Laundering, Drugs, and Terrorist Financing: HSBC Case History, at 210, July 16, 2012.
[50] *See* Department of Justice, Press Release, "BNP Paribas Agrees to Plead Guilty and to Pay $8.9 Billion for Illegally Processing Financial Transactions for Countries Subject to U.S. Economic Sanctions," June 30, 2014.
[51] See FinCEN, In the Matter of Doha Bank, New York Branch, New York, New York, No. 2009-1, April 20 2009; FinCEN, In the Matter of The Federal Branch of Arab Bank, PLC, New York, New York, No. 2005-2, August 17, 2005.
[52] For example, in its deferred prosecution agreement with the DOJ, HSBC noted that it had increased AML compliance spending nine –fold and AML staffing ten-fold between 2009 and 2011. *See* HSBC Bank USA, N.A. and HSBC Holdings plc DPA, ¶ 5, December 11, 2012.

(often limited) recordkeeping requirements of funds transfer systems in different countries, increase the likelihood that funds associated with illicit finance, including TF, may flow through these accounts and into the U.S. financial system. These relationships could potentially indirectly expose a U.S. financial institution to risk, including TF, if the foreign financial institution does not effectively implement AML/CFT controls.

To help mitigate against this risk, certain U.S. financial institutions are required to conduct due diligence on their foreign correspondents to ensure that the foreign correspondent's controls are adequate to manage the risk to the U.S. financial institution associated with this relationship.[53] These U.S. financial institutions are also required to conduct enhanced due diligence on certain higher risk foreign correspondents which requires (1) enhanced scrutiny, (2) determining whether the foreign correspondent maintains nested accounts for other foreign banks, and (3) the collection of beneficial owner information regarding foreign correspondents that are not publicly traded.[54] In addition to these requirements for foreign correspondents, U.S. financial institutions are also prohibited from maintaining correspondent accounts for foreign "shell banks" (*i.e.*, foreign banks with no physical presence in any country).[55]

Despite these requirements, there have been isolated and particularly egregious instances of U.S. banks not adequately managing potential TF risks posed by their relationships with foreign financial institutions. In one case, the U.S. subsidiary of a foreign parent bank was found to have failed to collect or maintain customer due diligence information on non-U.S. banking affiliates of the foreign parent bank for which it maintained correspondent accounts.[56] This resulted in transactions flowing to and from the United States without appropriate monitoring and alerts to identify movements of funds.[57] A significant number of non-U.S. financial institutions and their customers gained indirect access to the U.S. financial system without appropriate safeguards.[58] These customers included foreign banks that were publicly associated with terrorist organizations or terrorist financing.[59]

Cash Smuggling

As robust implementation of AML/CFT controls across financial institutions has raised the costs, risks and difficulty for TF networks operating within the financial system, cash smuggling has become an increasingly attractive way for foreign terrorists to transfer funds. The use of cash is attractive to criminals mainly because of its anonymity, portability, liquidity and lack of audit trail.

---

[53] *See* 31 C.F.R. § 1010.610(a); FFIEC BSA/AML Manual, pp. 177-80.
[54] *See* 31 C.F.R. § 1010.610(b).
[55] *See* 31 C.F.R. § 1010.630.
[56] *See* FinCEN, In the Matter of HSBC Bank USA, N.A. Mclean, Virginia, No. 2012-02, December 10, 2012.
[57] *Id.*
[58] *Id.*
[59] *See* Senate Permanent Subcommittee on Investigations, U.S. Vulnerabilities to Money Laundering, Drugs, and Terrorist Financing: HSBC Case History, at 225, 228, July 16, 2012.

According to the surveyed cases, since 2007, 18 TF-related prosecutions in the United States have in some way involved the use of cash to transfer funds to terrorist organizations. These cases have involved various FTOs, including core AQ, AQ in Iraq (the predecessor organization to ISIL), AQAP, Al-Shabaab, Hizballah, and FARC. There have been several notable cases in which U.S.-based individuals sought to smuggle cash for the benefit of Hizballah by concealing it in vehicles. On May 21, 2012, an individual was sentenced to more than six years in prison for conspiring to send hundreds of thousands of dollars to Hizballah.[60] His wife and co-conspirator previously pleaded guilty to one count of conspiracy to provide material support and resources to an FTO. During multiple meetings with an FBI confidential source, the two defendants discussed ways to secretly send money to Hizballah leaders in Lebanon.[61] The two defendants, after discussing multiple options to transfer the funds, ultimately agreed to send approximately $500,000 by concealing it inside a car, which they planned to send to Lebanon via a container ship, demonstrates how terrorist supporters were compelled to resort to cash smuggling – a less efficient means of funds transfer – in an effort to avoid U.S. controls.[62]

Similarly, on July 31, 2012, a Virginia resident pled guilty to attempted money laundering for placing what he believed to be $100,000 belonging to Hizballah inside a Jeep in 2010 and directing it to be shipped to Beirut; his arrest was the result of an FBI-orchestrated sting operation.[63] In a similar case, two Iraqi nationals pleaded guilty to TF-related charges resulting from an FBI-led sting operation.[64] From September 2010 through May 2011, one Iraqi participated in ten separate operations to send weapons and money that he believed was destined for terrorists in Iraq. In January 2011, he recruited the second defendant to assist in these material support operations. Over the course of the conspiracy, the individual believed he had sent $375,000 cash alone and $565,000 cash with the help of the second defendant. The primary means of smuggling the cash was in a hidden compartment of a tractor-trailer which would then be sent on to Iraq.[65]

These case studies demonstrate that cash couriers are being used to transfer funds to terrorist organizations. The U.S. government, particularly LEAs, proactively investigates and prosecutes such cases of abuse in order to effectively mitigate the vulnerability. For example, DHS, through ICE and CBP, has established special programs and initiatives to target bulk cash smuggling across U.S. borders.[66] DOJ and other prosecutorial authorities have levied criminal penalties for failing to report the cross-border transfer of currency in

---

[60] FBI, Press Release, "Ohio Man Sentenced to 75 Months in Prison for Scheme to Send Money to Hizballah," May 21, 2012. Available at http://www.fbi.gov/cleveland/press-releases/2012/ohio-man-sentenced-to-75-months-inprison-for-scheme-to-send-money-to-hizballah.

[61] *See United States v. Hor and Amera Akl*, No. 3:10-cr-00251-JGC, (N.D. Ohio, filed June 7, 2010).

[62] *Id.*

[63] *See United States v. Mufid Kamal Mrad*, Case No. 1:12mj363 (Affidavit) (E.D. Va. May 30, 2012); *see also* FBI, Press Release, "Vienna Man Pleads Guilty to Attempted Money Laundering," July 31, 2012.

[64] *United States v. Alwan et al*, Case No. 1:11-cr-00013 (Indictment) (W.D. Ky. 2011); Department of Justice, Press Release, "Iraqi National Pleads Guilty to 12-count Terrorism Indictment in Kentucky," August 21, 2012.

[65] *Id.*

[66] *See* Department of Homeland Security, Disrupt Terrorist Financing. Available at http://www.dhs.gov/topic/disrupt-terrorist-financing.

excess of $10,000.[67] Additionally, as detailed in the National ML Risk Assessment, the misuse of cash is limited by transaction record keeping and reporting requirements that require financial institutions to verify a customer's identity and retain records of certain information prior to issuing or selling payment instruments when purchased with currency in amounts between $3,000 and $10,000.[68] For cash transactions above $10,000, whether a single transaction or a series of related transactions with a customer in a single business day, financial institutions are required to file a CTR with FinCEN.[69] Other non-financial businesses must report cash transactions of more than $10,000 to the IRS and FinCEN.[70]

Cyber Security of the U.S. Financial Sector

Introduction

In its latest Worldwide Threat Assessment, the U.S. Intelligence Community stated "[c]yber threats to US national and economic security are increasing in frequency, scale, sophistication, and severity of impact."[71] The U.S. financial services sector in particular has been identified as a prime target for sophisticated and organized cyber attacks.[72] The increase in the frequency and breadth of attacks on banks can be attributed to banks holding not only money but also sensitive personally identifiable information and clients' intellectual property.[73] In light of this trend, the financial sector is considered to be one of the most experienced industries at dealing with cyber attacks.[74] The Financial Services Information Sharing and Analysis Center (or FS-ISAC) is the primary industry forum for collaboration on critical security threats facing the global financial services sector and has grown increasingly operational.[75]

Nation-states are commonly considered to be the most significant cyber threat, due to their resources and sophistication. The financial services sector in particular is at an increased risk, relative to other sectors, of sustaining cyberattacks by state actors.[76] In 2014, Russian hackers with connections to the Russian government, conducted one of the largest data breaches of a U.S. corporation when they compromised JP Morgan's servers and exposed the information of 83 million households and businesses.[77] In 2012, over the

---

[67] *See* 31 U.S.C. § 5332.
[68] *See* 31 C.F.R. § 1010.415.
[69] *See* 31 U.S.C. § 5313.
[70] *See* 31 U.S.C. § 5331 and 26 U.S.C. § 6050I.
[71] Worldwide Threat Assessment: hearing Before the Senate Armed Services Committee, 114th Cong. (2015), http://www.dni.gov/files/documents/Unclassified_2015_ATA_SFR_-_SASC_FINAL.pdf.
[72] *See A Global Perspective on Cyber Threats: Hearing Before the House Committee on Financial Services, Subcommittee on Oversight and Investigations*, 144th Cong. (2015) (Statement of Michael Madon, Board of Advisors Member, Center on Sanctions and Illicit Finance, FDD, at 2).
[73] *Id.*
[74] Hannah Kuchler, "US Financial Industry Launches Platform to Thwart Cyber Attacks," *Financial Times* (September 24, 2014), *available at* http://www.ft.com/intl/cms/s/0/080092b2-437a-11e4-8a43-00144feabdc0.html#axzz3dGyfOmYz.
[75] *See* Madon, *supra* note 96.
[76] *See* Briefing by the Congressional Research Service, May 28, 2015.
[77] Matthew Goldstein, Nicole Perlroth, and David E. Sanger, "Hackers' Attack Cracked 10 Financial Firms in

course of nine months, the Cyber Fighters of Izz ad-din Al Qassam, an activist group sponsored by Iran, targeted major U.S. banks with the largest distributed denial of service (DDoS) attack in history.[78] In 2013, North Korea launched an attack against the South Korean banking system, known as operation "Dark Seoul" that destroyed the information kept on an estimated 48,000 computers.[79]

Terrorist Organizations[80]

While terrorist groups are presently less sophisticated cyber-actors than either nation-states or most cybercrime syndicates, they nevertheless are becoming increasingly proficient in the cyber sphere and have an avowed interest in developing their capabilities. It is no surprise that terrorists are interested in cyberattacks since they are an especially effective method of asymmetrical attack. Cyberterrorism will likely never completely replace traditional terrorist attacks like bombings, but experts believe cyberattacks can be especially effective if used as a force-multiplier alongside them.[81] The risk from cyberterrorism attacks is particularly elevated for the financial sector. As a critical infrastructure and the heart of the U.S. economy, an attack on the financial sector would have an extremely high-impact. Moreover, the financial industry consists of many highly visible symbols of Western capitalism, which are appealing targets for terrorists.

Al Qaeda has expressed interest in "electronic jihad" as a means of disrupting the American economy, and Al Quaeda prisoners have revealed the group's intent to use cyberattacks.[82] Al Quaeda has probed the electronic infrastructure for ways to disrupt or disable critical infrastructure such as electric power, telephone communications, and water supplies.[83] ISIS, too, has announced a "cyber caliphate," though it has so far launched only low-impact website-defacement attacks.[84]

The Syrian Electronic Army (SEA), a group of computer hackers who support Syrian President Bashar Al-Assad, is known for targeting groups unsympathetic to the Assad regime. The SEA's early activity consisted of spamming sites with pro-Assad comments

---

Major Assault," *The New York Times* (October 3, 2014), *available at* *http://dealbook.nytimes.com/2014/10/03/hackers-attack-cracked-10-banks-in-major-assault/?_php=true&_type=blogs&_r=1*.

[78] Joseph Menn, "Cyber Attacks Against Banks More Severe Than Most Realize," *Reuters* (May 18, 2013), *available at* *http://www.reuters.com/article/2013/05/18/us-cyber-summit-banks-idUSBRE94G0ZP20130518*.

[79] *See* K.J. Kwon, "Smoking gun: South Korea uncovers northern rival's hacking codes," April 23, 2015, *available at* http://edition.cnn.com/2015/04/22/asia/koreas-cyber-hacking/index.html?eref=edition.

[80] Prepared Memo for *A Global Overview of Cybersecurity Threats*, 114th Cong. (2015)

[81] Suleymon Ozeren, "Cyberterrorism and International Cooperation," *Responses to Cyber Terrorism,* 72-73 (IOS Press 2008).

[82] *See* Thomas M. Chen, "Cyberterrorism After Stuxnet," *in Terrorism: Commentary on Security Documents, vol. 138, The Resurgent Terrorist Threat*, 16-17 (Douglas C. Lovelace Jr., ed. 2015) (article originally published in the United States Army War College Press, June 2014).

[83] *See* Chen, at 16-17.

[84] Emma Graham-Harrison, "Could Isis's 'cyber caliphate' unleash a deadly attack on key targets?" The Observer, April 12, 2015, *available at* http://www.theguardian.com/world/2015/apr/12/isis-cyber-caliphate-hacking-technology-arms-race .

and escalated to large scale DDoS attacks.[85] The SEA is perhaps most noted for claiming responsibility for hacking the Associated Press' Twitter account where it posted "Breaking: Two Explosions in the White House and Barack Obama is injured."[86] This act of cyber vandalism caused the Dow Jones Industrial Average to drop 150 points from 14697.15 to 14548.58.[87] While the market corrected itself within minutes, the fake tweet is estimated to have erased $136 billion in equity market value.[88]

Although it is widely believed that terrorists do not yet have the capabilities to launch destructive or even disruptive cyberattacks, the means of doing so are becoming increasingly cheap and accessible. It costs less than a thousand dollars to purchase a botnet capable of disruptive DDOS attacks, and renting the same system costs only a few dollars an hour.[89] While the capabilities to mount destructive attacks and cyberterrorism are more expensive to mount, the price is dropping. Moreover, terrorists can easily hire the services of sophisticated cyber mercenaries at any time. "Guns-for-hire" who offer their hacking services on the black market can be highly sophisticated; for example, "Hidden Lynx" is a group of hackers-for-hire believed to be behind successful cyberattacks on over 100 organizations including U.S. defense contractors and investment banks.[90]

Looking further down the road, terrorists could begin to draw cyber-capabilities from nation-states just as they draw other types of support from nation-states. As nation-states friendly to terrorist organizations improve their cyber-capabilities, the risk of terrorists gaining access to sophisticated cyber-weapons or beneficial information increases.[91] For example, Iran is a major exporter of terrorism, and its Islamic Revolutionary Guard Corps is known to have provided Hezbollah with (non-cyber) training.[92] Iran could begin providing terrorists cyber-training, or simply offer them a map

---

[85] Andrea Peterson, "The Post Just Got Hacked by the Syrian Electronic Army. Here's Who They Are," *The Washington Post* (August 15, 2013), *available at* http://www.washingtonpost.com/blogs/the-switch/wp/2013/08/15/the-post-just-got-hacked-by-the-syrian-electronic-army-heres-who-they-are/.

[86] Max Fisher, "Syrian Hackers Claim AP Hack That Tipped Stock Market by $136 Billion. Is it Terrorism?" *The Washington Post* (April 23, 2013), *available at* http://www.washingtonpost.com/blogs/worldviews/wp/2013/04/23/syrian-hackers-claim-ap-hack-that-tipped-stock-market-by-136-billion-is-it-terrorism/

[87] *Id.*

[88] *Id.*

[89] Nick Clayton, "Where to Rent a Botnet for $2 an Hour or Buy one for $700," Wall Street Journal, November 5, 2012; http://blogs.wsj.com/tech-europe/2012/11/05/where-to-rent-a-botnet-for-2-an-hour-or-buy-one-for-700/ .

[90] *See* Thomas M. Chen, "Cyberterrorism After Stuxnet," *in Terrorism: Commentary on Security Documents, vol. 138, The Resurgent Terrorist Threat*, 19 (Douglas C. Lovelace Jr., ed. 2015) (article originally published in the United States Army War College Press, June 2014).

[91] *See* Thomas M. Chen, "Cyberterrorism After Stuxnet," *in Terrorism: Commentary on Security Documents, vol. 138, The Resurgent Terrorist Threat*, 19 (Douglas C. Lovelace Jr., ed. 2015) (article originally published in the United States Army War College Press, June 2014).

[92] *See* The Future of Homeland Security: Evolving and Emerging Threats: Hearing Before the Senate Committee on Homeland Security & Governmental Affairs 112th Cong., 2012, at 4 (Statement of Frank J. Cilluffo) *available at* http://www.hsgac.senate.gov/hearings/the-future-of-homeland-security-evolving-and-emerging-threats .

of any vulnerabilities it has found in U.S. cyber-defenses.[93] While it does not appear to have happened yet, depending on the political situation and its willingness to share information, a nation-state could expand its proxies and partners from hacktivists and criminals to terrorist groups, and thereby catapult terrorists' cyber sophistication to lethal new levels.

[93] *C.f.* Briefing by Illan Berman for the Majority staff of the House Financial Services Committee, May 27, 2015.

Witness Biographies

Cyrus Vance, Jr., District Attorney, New York County District Attorney's Office

Cyrus R. Vance, Jr., was first sworn in as the District Attorney of New York County on January 1, 2010. Over the following four years, Mr. Vance enhanced the District Attorney's Office as a national leader in criminal justice by expanding its expertise on an array of 21st century crimes. Mr. Vance's many achievements as District Attorney include the takedown of violent street gangs, dismantling domestic and international cybercrime and identity theft operations, the first local terrorism convictions in New York State courts, and the recovery of billions of dollars from international financial institutions that had been engaged in violating international sanctions.

District Attorney Vance was reelected in 2013. Mr. Vance is the co-founder and co-chair of Prosecutors Against Gun Violence, an independent, non-partisan coalition of prosecutors from major jurisdictions across the country which will identify and promote prosecutorial and policy solutions to this national public health and safety crisis. In recent months, District Attorney Vance has taken a national leadership role in addressing the issue of race in the criminal justice system, including commissioning a study by the non-partisan Vera Institute of Justice to evaluate the office's practices in charging, plea-bargaining, and bail. Mr. Vance, using funds obtained through the sanctions cases against international financial institutions, has also made significant investments in a series of transformative criminal justice initiatives in New York City and nationally. These programs include equipping every NYPD officer and patrol car with handheld mobile devices and tablets, eliminating the national rape kit backlog, reducing the number of individuals with behavioral health issues in the criminal justice system, and enhancing security in NYCHA developments throughout the city.

Chip Poncy, Founding Partner, Financial Integrity Network

Prior to launching the Financial Integrity Network, Mr. Poncy served as the interim Head of Financial Crimes Compliance for Mexico and the Latin American region for one of the world's largest banks, assisting in the development and implementation of an enterprise-wide financial crimes compliance program adherent to global standards.

From 2002-2013, Mr. Poncy served as the inaugural Director of the Office of Strategic Policy for Terrorist Financing and Financial Crimes (OSP) and a Senior Advisor at the U.S. Department of the Treasury. As the Director of OSP from 2006-2013, Mr. Poncy led an office of strategic policy advisors in creating policies and initiatives to combat the full spectrum of illicit finance, including money laundering, terrorist financing, WMD proliferation financing, and kleptocracy flows. As a Senior Advisor from 2002-2006, Mr. Poncy assisted Treasury leadership in developing the U.S. Government's post-9/11 strategy to combat terrorist financing. He also assisted senior leadership in creating and developing the Office of Terrorism and Financial Intelligence in the post-9/11 government reorganization.

Mr. Poncy led the U.S. delegation to the Financial Action Task Force (FATF) from 2010-2013, co-chaired the policy working group of the FATF from 2007-2013, and managed U.S. participation on various G7, G8 and G20 illicit finance experts groups from 2008-2013. Key accomplishments in these roles included assisting in the revision and adoption of the FATF's global standards and assessment processes for future jurisdictional reviews under the FATF global network, and facilitating the integration of counter-illicit finance into the broader global financial reform agenda since 2008.

Mr. Poncy began his career as an associate in the New York offices of the law firm White & Case and has served as general counsel to biotechnology and internet radio companies. He has co-pioneered a graduate course on national security and the international financial system as an adjunct associate professor at Georgetown University's Edmund A. Walsh School of Foreign Service. Mr. Poncy graduated with honors from Harvard University (Bachelor of Arts in Government) and The Johns Hopkins School of Advanced International Studies (Masters of Arts in International Relations) and holds a Juris Doctor from the Georgetown University Law Center.

John W. Carlson, Chief of Staff, Financial Services Information Sharing and Analysis Center

John W. Carlson is chief of staff of the Financial Services Information Sharing and Analysis Center (FS-ISAC). The FS-ISAC is a member-owned non-profit created in 1999 to share timely, relevant and actionable physical and cyber security threat and incident information to improve the overall security posture of the financial services sector.

Prior to joining the FS-ISAC, Carlson served as the Executive Vice President of BITS, the technology and policy division of the Financial Services Roundtable. At BITS, Carlson led cybersecurity, technology risk and collaboration programs for a total of 12 years and participated in the Financial Services Sector Coordinating Council (FSSCC), where he continues to serve on the Executive Committee. Carlson served as a Managing Director of Morgan Stanley's operational risk department in 2010-11, and in a variety of leadership roles at the Office of the Comptroller of the Currency (1993-2002), U.S. Office of Management and Budget (1990-93), Federal Reserve Bank of Boston (1988-90), and United Nations Center for Human Settlements (1986). Carlson holds a Masters in Public Policy from the Kennedy School of Government at Harvard University and a B.A. from the University of Maryland, where he served on the Board of Regents.