MONEY LAUNDERING
AND TERRORIST ACTIVITY FINANCING WATCH

April-June 2011

UNCLASSIFIED

ISSN: 1923-8282

Financial Transactions and Reports Analysis Centre of Canada

Centre d'analyse des opérations et déclarations financières du Canada

Canada

Money Laundering and Terrorist Activity Financing Watch:

- Summarizes relevant group-based, activity-based and country-based money laundering (ML) and terrorist activity financing (TF) issues;
- Alerts readers to new developments that could possibly be exploited for money laundering or terrorist activity financing purposes in Canada.

The ML/TF Watch is a quarterly review of news articles compiled by FINTRAC's Macro-Analysis and Research unit. The articles provided in this issue range from April 1, 2011 to June 30, 2011.

Caveat

The content presented herein is a summary of news articles and does not include any FINTRAC analysis. The views expressed are those of the original authors. FINTRAC is not responsible for the accuracy, currency or the reliability of the content. References to the respective articles are provided at the end of this document.

Money Laundering

Terrorist Activity Financing

Money Laundering

GROUP-BASED

FARC affiliates convicted for money laundering: Three Colombian men were convicted by a U.S. federal jury for drug trafficking and money laundering charges on May 4th. The defendants, Miguel Antonio Jimenez Torres, Hector Fabio Zapata Alvarez and Nivaldo Riascos Renteria were also identified as affiliates of the Revolutionary Armed Forces (FARC), the paramilitary group currently controlling the South American cocaine trade. Prosecutors alleged that the three arranged to smuggle a shipment of 10 tons of cocaine into the south-western United States through Ecuador and Mexico. According to a *Thomson Reuters* article, more than US$491,000 was wired from a FARC-affiliated cartel to a U.S. undercover agent in Seattle as a down payment for the shipment. The jury convicted the three defendants over arranging the payments and transportation of the drugs, which never made it to the United States. Emily Langlie, spokeswoman for the U.S. Attorney in Seattle, explained that 10 tons of cocaine has a street value of about US$100 million or an equivalent of 10 million user doses. According to the trial testimony, the planned cocaine shipment, which was to be concealed in ballast tanks of cargo vessels, was disrupted by a Colombian army raid in early 2008 on a FARC campsite near Ecuador in which the FARC leader, Paul Reyes, was killed. Sentencing is scheduled for August 8, 2011; Jimenez and Zapata face a 10-year minimum prison sentence while Riascos faces at least 20 years in prison for a prior drug trafficking conviction in New York State.[1]

FINANCIAL ACTIVITY-BASED

UN report cites Canada as major source for synthetic drugs: The United Nations' World Drug Report for 2011, released on June 2nd, claimed that Canada is a major source for synthetic drugs like ecstasy and methamphetamines (MDMA). The report, which is based on global police, government and health records, also states that Canada is the leading exporter of meth to the United States, the Philippines, Malaysia, Mexico and Jamaica. Additionally, the report states that it was ecstasy production in Canada and subsequent smuggling that fuelled "the resurgence" of ecstasy use south of the border. According to a *Globe and Mail* article, Canada is considered to have loose regulations over the import and domestic trade of precursor chemicals, like pseudoephedrine. The article however, states that on June 2nd a new Canadian law was introduced, making it illegal to possess precursor chemicals and equipment that produce synthetic drugs. The head of the Royal Canadian Mounted Police's (RCMP) drug squad in British Columbia, Brian Cantera, states that organized crime groups in Canada that have ties to India and China can bring in large quantities of precursor chemicals needed to produce synthetic drugs in underground laboratories set up across the country. Also, labs found in Canada are described as "large-scale productions" that use very sophisticated equipment as opposed to the small "stove-top" meth operations found in the United States. According to the UN report, Canadian authorities shut down a dozen ecstasy labs and 23 meth labs in 2009, seizing nearly half a metric ton of ecstasy.

Furthermore, on May 25th, police in British Columbia shut down a major drug ring that was operating "super labs" to produce methamphetamines and ecstasy at several

locations, including Kamloops and Surrey. According to the RCMP, the drug ring, which involved several organized crime groups such as Eastern European organized crime, was also producing equipment to set up eight more mobile labs. In addition to the drug-making equipment and chemicals, police also seized 32 firearms and $1 million worth of stolen property.

In a similar incident, two Ontario women were held by U.S. authorities on May 10th after Detroit customs officers found more than 75,800 ecstasy pills hidden in their vehicle at the Ambassador Bridge. The total weight of the drugs was estimated at 24 kilograms (53 pounds), making it the largest ecstasy seizure by U.S. Customs at the Ambassador Bridge since 2009. According to the National Drug Intelligence Center, MDMA production in Canada is high and possibly increasing, causing a rise in MDMA smuggling through the U.S.-Canada border. The drug intelligence center also stated that Canadian-based Asian drug trafficking operations are producing the drugs for distribution in the United States.[2]

Ministry of Public Security statistics reveal an increase in bank card cloning and Internet fraud in Quebec: Statistics reported by the Ministry of Public Security in Quebec on Internet fraud and the cloning of debit cards revealed a significant increase of reported cases of fraud in Quebec. In a study entitled "Études des Crédits" (Study of Credits) and presented by the Ministry to the National Assembly of Quebec on April 21st, statistics revealed that between 2008 and 2009, the number of cases in Quebec concerning debit and credit card cloning increased from 95 to 265. In 2008, 60 cases alone totalled $120,000 while in 2009, 123 cases totalled $341,000 in fraudulent money. The study also found that fraud via the Internet has increased considerably. For example, there was a 44% increase of reported cases between 2008 and 2009 with the total amount of fraudulent money obtained through Internet fraud also increasing from $843,000 in 2008 to $980,000 in 2009. The Ministry of Public Security produced its statistics from incidents reported to the municipal police, La Sûreté du Québec, and the native police.

A recent example of debit card fraud occurred in early April when investigators of Quebec's Fraud Unit arrested three individuals from Montreal after discovering their debit fraud scheme. The three men would enter different stores or restaurants; distract cashiers and replace the debit card machines at the counters with ones that register all bank card information, including their PIN numbers. The criminals would return to switch back the devices and leave with the machines holding the registered credit and debit card information.[3]

U.S. Justice Department targets the three largest online gambling companies: On April 15th, the founders of the three top online gambling companies—PokerStars, Full Tilt Poker, and Absolute Poker—were charged with bank fraud, money laundering and illegal gambling by the U.S. Department of Justice. Prosecutors have obtained restraining orders against 75 bank accounts in 14 countries and now seek a total of US$3 billion in forfeitures and fines from the three online gambling businesses, along with the financial firms and individuals complicit with processing the bets. In total, 11 individuals (of which eight are U.S. citizens and nine live in Costa Rica, Ireland, Canada and the Isle of Man) were indicted by the Department of Justice for allegedly operating or helping the online gambling sites operate against the *Unlawful Internet Gambling Enforcement Act (UIGEA)*. Established in October of 2006 in the United

States, the UIGEA prohibits online gambling businesses and financial institutions from handling funds related to online bets or wagers. The three companies, which are located offshore, nevertheless continued their operations in the United States. According to an article from *moneylaundering.com*, because many U.S. financial institutions were unwilling to process bets or payouts from the three online gambling businesses, the companies used various methods to evade the UIGEA and deceive these institutions into processing online gambling payments. According to the indictment, the online gambling companies relied on several "well-paid" payment processors to deceive U.S. banks and obtain accounts for the poker companies. The payment processors, who were all charged in the indictment, lied to banks such as Citibank, Wells Fargo and Fifth Third Bank by disguising money received from U.S. gamblers as payments to hundreds of non-existent online sellers for merchandise such as jewellery and golf balls. In another case, in order to circumvent rules imposed by Visa and MasterCard requiring member banks to identify transactions involving Internet gambling operations, the payment processors lied to banks by creating dozens of fake businesses to act as transaction beneficiaries. PokerStars, Full Tilt Poker and their payment processors also convinced smaller, local banks facing financial problems to knowingly accept illegal wires tied to online gambling funds. For example, the Vice Chairman of the board of SunFirst Bank in Utah agreed to process gambling transactions in return for a US$20,000 bonus and a US$10 million investment in the bank. By November 2010, SunFirst Bank had processed more than US$200 million in payments for Poker Stars and Full Tilt Poker. The gambling companies also directed players to purchase stored value debit and phone cards and advertized these methods as online legitimate payment products to place bets with the companies. According to the FBI statement, nearly one-third or more of the billions of dollars in payment transactions that U.S. banks were deceived into processing went directly to the poker companies as revenue from the fee charged to players on almost every game played online. The United States also seized five websites used by the gambling companies to operate their illegal online businesses in the United States.

The charges against the online gambling companies were not limited to the United States alone. On June 29th, Full Tilt Poker was completely shut down after its gaming license was revoked by the Alderney Gambling Control Commission (AGGCC), an independent organization that regulates online gambling in parts of Europe. Since the revocation, users across the world, including Canada, are no longer able to access the website. According to an article by the *Journal de Montréal*, the Full Tilt website had attracted some 295,000 visitors from Canada since May 2010. In Quebec alone, 80,000 downloaded the game application from the website while 33,000 visited the website.[4]

FBI identifies incidents of cyber criminals hacking bank accounts: The U.S. Federal Bureau of Investigation (FBI) has identified 20 incidents, between March 2010 and April 2010, of cyber criminals hacking bank accounts in the United States and sending unauthorized wire transfers to Chinese economic and trade companies. The hackers specifically targeted the bank accounts of small-to-medium size businesses, stole approximately US$11 million and attempted to wire about US$20 million in stolen funds. The intended recipients of the illegal transfers were companies registered in port cities near the China-Russia border. According to the FBI, the scheme typically involved company

computers used to transfer funds which were compromised with malware that captured corporate online banking credentials. Afterwards, the hackers were able to send anywhere from US$50,000 to US$985,000, with most transfers above US$900,000. Investigators are still unable to identify who is responsible for these transfers and whether the Chinese accounts were the final destination of the funds or if they were forwarded elsewhere. According to FBI authorities, cyber criminals are increasingly using similar techniques to gain access to bank accounts and to steal money.[5]

Baltimore drug traffickers charged with money laundering: On April 27th in Baltimore, Maryland, Steven Blackwell and Joy Edison were accused by federal prosecutors for laundering the profits of a heroin-selling operation through the Maryland State Lottery, Las Vegas casinos and a local used-car dealership. According to the indictment, since December 2003, Blackwell and Edison distributed more than a kilogram of heroin in Maryland, New York, and the Dominican Republic, generating millions of dollars in income. The indictment further detailed the methods in which Blackwell and Edison laundered their illicit proceeds. In one scheme, the two defendants purchased winning Maryland State Lottery tickets from the actual winners and collected the money from the lottery agency. While the indictment does not revel exactly how Blackwell and Edison found the lottery winners and purchased their tickets, it indicated that Blackwell purchased the tickets for US$5,000 each and, in a five week period, cashed them in to receive three cheques from the Maryland State Lottery for a total of US$15,000. The indictment also alleges that money was laundered through Las Vegas casino chips, including up to US$35,000 worth of chips from the Venetian Resort. In another scheme, Blackwell and Edison laundered their heroin proceeds by purchasing residential and investment properties through two real estate companies controlled by them named JJM Realty LLC. and J. Edison Properties. Blackwell and Edison also purchased luxury and consumer items and laundered large sums of money through a car dealership. According to the *Baltimore Sun*, Blackwell is considered by prosecutors to be one of Baltimore's most notorious drug dealers and has been at the center of the drug trade in the city. Although police suspected Blackwell of being one of the city's biggest drug dealers for years, he was not arrested until August 2010. Federal authorities are now demanding the forfeiture of US$10 million from Blackwell and all properties purchased with illicit drug proceeds.[6]

Cases of academic sector being used for money laundering: On April 28th, the President of California's Tri-Valley University, Xia-Ping "Susan" Su, was charged with transactional money laundering, visa fraud, and harboring undocumented immigrants. The U.S. Immigration and Customs Enforcement and the Department of Homeland Security accused Su of running her university as a front for illegal immigration. The unaccredited online university was founded by Su in 2008 with 95% of its students being foreigners from India. A 22-page indictment by the federal jury of Oakland, California, states that Su is accused of operating a visa fraud scheme where she took advantage of foreigners wishing to study in the United States. Court documents indicated that Su's scheme involved submitting fraudulent documents to the Department of Homeland Security to unlawfully obtain study visas for foreign students. Furthermore, the indictment alleges that in Su's visa fraud scheme, she received millions of dollars in tuition fees and that she engaged in several money laundering

transactions totaling US$3.2 million. A separate civil lawsuit states that students were charged US$2,700 per semester and by September 2010, the university catered to 1,555 students, providing an estimated revenue of nearly US$4.2 million for that semester alone. According to the indictment, between February 2009 and September 2010, Su received US$1,159,656 in PayPal transactions and US$1,776,036 in credit card payments, in addition to smaller amounts of cash and wire transfers. Su also engaged in a pyramid scheme where enrolled students could collect up to 20% of the tuition of new students whom they referred to the university. The pending lawsuit over Su seeks forfeiture of five properties which were allegedly purchased with fraud proceeds.

In a related story on the use of the academic sector for fraud and money laundering, on April 13th, a federal grand jury indicted Poul Thorsen, a Danish doctor who allegedly stole more than US$1 million in grant money from the U.S. Center for Disease Control and Prevention (CDC). According to the indictment, between 2000 and 2009 the CDC awarded a grant of more than US$11 million to two governmental agencies in Denmark for autism studies to be administered by various Danish institutions, including Aarhus University. Thorsen was assigned as the principal investigator of the CDC grant. As such, in 2002, Thorsen moved back to Denmark to take on the position of administrating the research money on behalf of the CDC. Thorsen also held a faculty position at Aarhus University where scientists performed research under the grant. The indictment further states that between February 2004 and June 2008, Thorsen fraudulently reimbursed grant money by submitting over a dozen fake invoices to Aarhus University which falsely stated that work had been done and expenses were owed in connection to the grant. Thorsen allegedly instructed Aarhus University to pay the invoices by transferring the grant money to CDC Federal Credit Union bank accounts in Atlanta, Georgia. As such, Aarhus University transferred hundreds of thousands of dollars to the bank accounts under the impression that they belonged to CDC when in fact they were personal accounts of Thorsen. According to prosecutors, once the money was transferred, Thorsen withdrew the funds and purchased a house in Atlanta, a Harley Davidson motorcycle, luxury vehicles, and numerous cashiers' cheques. Thorson could face decades in prison if convicted on all charges including 13 counts of wire fraud and nine counts of money laundering.[7]

Bitcoins: a new anonymous digital currency and a potential vehicle for criminals to transfer money: According to investigators, an emerging digital currency named "Bitcoin", intended to allow people to send money without the use of payment processors or other financial institutions, could also be a method used by criminals to make anonymous international transactions. Bitcoin is an open-source digital currency created in January 2009 by Satoshi Nakamoto. An article by *Time* magazine claims that the currency can be exchanged "untraceably" between two people across borders, making it the world's first distributed and anonymous currency. Bitcoins are generated by a computer algorithm from software that anyone can download and install on any computer. Once the Bitcoin software has been installed, a user can generate, store and directly exchange Bitcoins with others without the verification of a third party such as a bank or government. However, the process of generating or "mining" Bitcoins generally requires powerful computers to calculate the intensive algorithms. As such, *Thomson Reuters* explains that users have the option of

purchasing Bitcoins from Bitcoin exchangers that operate around the world in countries like the United Kingdom, Poland, Japan and elsewhere. These exchangers allow users to buy Bitcoins with "real-world" money. The exchangers have bank accounts at financial institutions where they receive and send payments whenever users buy or sell Bitcoins. *Thomson Reuters* also adds that Bitcoin exchange businesses are not regulated because it is uncertain if they should be considered money transmitters or some form of a financial institution; making the obligation to report suspicious activity unclear. Additionally, governments cannot regulate bank intermediaries for Bitcoin transactions because none are used to trade Bitcoins. Finally, the Bitcoin software, which acts as a peer-to-peer network, contains a database of transactions, allowing a record to be kept of all transfers. However, the transactions are cryptic, meaning there is no way to identify who sent money to whom just by looking at the master list of Bitcoin transactions.

On June 6th, two U.S. senators released a letter to the Department of Justice and the Drug Enforcement Administration (DEA) calling on federal authorities to shut down the "untraceable" digital currency, claiming that it is an "online form of money laundering" for drug traffickers and those who are looking to conceal the source of their money. In their letter, the senators cited information from press reports suggesting that some tech-savvy individuals were accessing a website called *Silk Road*, an underground marketplace that allows users to anonymously purchase and sell illegal drugs such as cocaine, heroin, ecstasy, and marijuana. The senators' letter indicates that the website only accepts Bitcoin as a method of payment for the illegal purchases and, once a payment has been made, the drug sellers use the U.S. Postal Service to mail the drugs to the buyer. According to *Thomson Reuters,* Bitcoin enthusiasts are concerned that the DEA might close down the bank accounts of the Bitcoin exchangers and seize their funds in response to the senators' letter and the drug trafficking allegations regarding *Silk Road*. Nonetheless, some participants on a Bitcoin discussion forum speculated that if the U.S. government were to ban transactions with Bitcoin exchange businesses, a "layer of shell companies" would appear with methods that are harder to track in order for them to continue their business—a similar outcome to what happened when U.S. financial institutions were prohibited from processing online gaming transactions.

In June 2011, Bitcoin experienced two major hacks; first, a hacker transferred 25,000 Bitcoins—at the time worth almost US$500,000; second, an attack on a Bitcoin exchange business in Japan involving more than 400,000 Bitcoins which were worth almost US$9 million dollars. The attempt to sell off the coins at once was a sale so substantial that it caused the value of Bitcoins to drop to US$0.01 and trading on the Mt Gox site was suspended. Prior to the hack, more than 6.5 million Bitcoins were in circulation for approximately US$27 each, making the total value of Bitcoins US$180 million. [8]

COUNTRY-BASED

Public whistleblower program to counter money laundering in Mexico: The Mexican attorney general's office announced a whistleblower program on April 4th to reward those who report suspected money laundering by allowing them to receive up to one-quarter of the illicit funds or property seized. The initiative is intended to target the financial operations of drug cartels through the participation of Mexican citizens as whistleblowers. Those witnessing suspicious

financial transactions can report their concerns in person, by telephone or via e-mail. While Mexican citizens will be eligible for monetary rewards that are determined on case-by-case basis, law enforcers, public officials and banking system employees are exempted from compensation because, in part, their profession already requires them to track suspicious transactions. The new program, according to *Thomson Reuters*, is based on the premise that the public will want to report instances of possible money laundering by drug cartels because there is now a financial incentive and the public is generally motivated to put an end to the violence that drug cartels cause. However, U.S. enforcement officials are sceptical about the success of the program due to the cartels' reputation for extreme violence, claiming it could deter the general public from reporting to the authorities over fear of violent retribution. According to the *Associate Press*, Mexico has struggled to find effective measures to combat a suspicious cash flow of approximately US$10 billion a year that is possibly linked to drug trafficking.[9]

Money laundering bill passed in Argentina: On June 1st, Argentina's Senate passed a law to strengthen financial controls and criminalize money laundering in the country. With the new bill, the government of Argentina will gain more power to freeze and confiscate property as well as an additional provision allowing Argentina to prosecute Argentines committing money laundering in other countries. The bill is in response to the warning Argentina received by the Financial Action Task Force (FATF) of potentially being included on its list of jurisdictions with strategic deficiencies to counter financial criminal activity. In response to Argentina's legal amendments, the FATF declared in a public statement that there are still several shortcomings in the country's anti-money laundering (AML) and counter-terrorist financing (CTF) regime, such as not adequately criminalizing terrorism financing as well as other significant AML/CTF deficiencies. The FATF will continue to closely monitor Argentina's ongoing progress and has given the country until October 2011 to make more substantial commitments. In efforts to avoid further international scrutiny, the government of Argentina also wants to find the billions of dollars in undeclared money held by Argentines. According to *Thomson Reuters*, Argentines are still hiding savings worth nearly US$10 billion to US$15 billion in safe-deposit boxes or under their mattresses a decade after bank deposits were frozen and devalued during a severe economic crisis. The figure represents 10% to 15% of total current deposits in the country and, in addition to the money stashed away, Argentines are estimated to have another US$150 billion in savings abroad.[10]

Report reveals how some corrupt Chinese officials launder money overseas: An article by *Thomson Reuters* on June 16th cites eight ways corrupt Chinese officials and company executives in China transferred illegal assets overseas. According to a report released by the Anti-Money Laundering Monitoring and Analysis Center, illegal assets were transferred overseas through legal and illegal channels. The eight main methods used included cash smuggling, underground banking services, trade under current accounts, overseas investment, credit cards, offshore financial centers, direct overseas payments and payments to family members or loved ones living overseas. The exact figure of the assets transferred overseas is unclear because Chinese officials charged for corruption began to flee the country at the end of the 1980s. The report, however, quoted statistics from the Chinese Academy of Social Sciences, revealing approximately up to 800 billion yuan (US$123 billion) had been

transferred overseas by fleeing or missing officials and company executives since the mid-1990s. The report explains that when these assets were transferred it caused considerable losses to the country because the money could not be recovered or found. Included in the report are findings on the different locations to which corrupt officials and businessmen fled. Officials with a high rank or large assets tended to flee to Western countries such as the United States, Canada, Australia, and the Netherlands while those with a lower rank or small assets found safe havens in neighbouring countries to China such as Thailand, Myanmar, Malaysia, Mongolia and Russia.[11]

Money laundering concerns involving public officials at Indonesia's Citibank: According to Indonesia's financial intelligence unit, PPATK, Indonesian public officials are possibly using Citibank's private banking unit in Indonesia for money laundering purposes. PPATK launched a money laundering investigation on April 18th after a high-value client manager at Citibank allegedly embezzled more than US$2 million from her private banking clients who were all members of the "Citigold" program, which requires customers to have a balance of at least 500 million Indonesian rupiah (US$59,000). A regulatory investigation revealed that the majority of the manager's clients were public servants with balances worth more than their expected salaries of 35 million rupiah (US$4,130) per month. The public officials' balances also exceeded the minimum requirements of the Citigold program. A *Thomson Reuters* article states that corruption in Indonesia is high, with the country ranked as 110th on the 2010 corruption perceptions index by Transparency International. This makes Indonesia one of the most corrupt countries in the world; causing suspicion over the source of the money held by the public officials in the Citigold accounts. In addition to investigating the source of the funds, PPATK is also assessing whether Citibank may have breached some of the country's anti-money laundering (AML) regulations with regards to domestic politically exposed persons (PEPs). According to the head of Kuala Lumpur's Anti-Money Laundering Network, Nigel Morris-Cotterill, like all major international banks, Citibank is particularly attractive for money launderers given it is a U.S. bank and therefore provides an "easy channel" to U.S. dollars and, ultimately, the United States. Morris-Cotterill also claims that Indonesia was formerly deemed a non-cooperative jurisdiction by the Financial Action Task Force, but has now reversed the situation and is on the "offensive" side with regards to money laundering and terrorist financing.[12]

Terrorist Financing

GROUP-BASED

Charity status of the Canadian branch of World Islamic Call Society revoked over links to Gadhafi: A Canadian charity formed in 1989 and based in London, Ontario, lost its charitable status on March 26, 2011 after it was revoked by the Canadian government. An article by the *Ottawa Citizen,* on May 5th, cited government documents claiming the World Islamic Call Society was established as a front for Moammar Gadhafi and has direct financial ties with the Libyan ruler. The documents indicated that U.S. money was wired from Gadhafi's "jihad fund" to the personal bank account of Assem Fadel, the president of the World Islamic Call Society's only office in Canada. After receiving the funds, Fadel would transfer the money from his personal account into the charity's Canadian bank account to be redistributed to known terrorist

organizations. For example, the documents revealed a payment of $170,814 made to Jamaat al-Muslimeen, a terrorist group known for "terror campaigns of rape, torture and murder." The *Ottawa Citizen* also cited documents by the Canada Revenue Agency which revealed that the Canadian charity transferred $10,000 directly to the terrorist group's leader, Yasin Abu Bakr. The government documents also claimed that the terrorist organization, which is linked to the 2007 bomb plot at John F. Kennedy International Airport, was funded by the Canadian branch of the World Islamic Call Society. According to the federal documents, Fadel also wired funds to individuals and organizations in the United States, Trinidad and Egypt. In an interview with the *Ottawa Citizen*, Fadel refuted the claim that the charity's money financed terrorism and explained that the reason he personally handled the money was because the charity does not have a U.S. bank account and, since the deposits were in U.S. funds, it was his responsibility to receive, transfer and redistribute the funds as directed by the head organization in Libya. Fadel also mentioned that he would not appeal the government's decision to revoke the registration of the charity, but rather the organization will continue without its charitable status, forcing the group to pay taxes and to no longer be able to issue tax deductible receipts. The *Ottawa Citizen* also stated that the charity's only donor was WICS-Libya, Gadhafi's umbrella organization formed in 1972, which he wires money to annually.[13]

New designation of Chechen group in North Caucasus by the United States: On May 26th, the United States added Caucasus Emirate, a Chechen group based in North Caucasus, to its list of designated terrorist groups. The U.S. State Department also authorized an award of up to US$5 million for information on the location of the group's leader, identified as Doku Umarov. Investigators claim that Umarov was the main organizer of a suicide bombing outside the Chechen Interior Ministry in May 2009. The group claimed responsibility for other several large-scale terrorist attacks as well. In early 2011, the group bombed the Domodedovo airport in Moscow, killing 36 people; in 2010 the group bombed the Moscow subway, killing 40 people; and in 2009 the group was responsible for the bombing of the high-speed Nevsky Express train, killing 28 people. The leader of the terrorist group, Umarov, has openly issued statements in the past encouraging a campaign of violence against his groups' enemies, which includes the United States, Israel, the United Kingdom and Russia. The State Department's coordinator for counter-terrorism, Daniel Benjamin, stated that the designation of Caucasus Emirate is in response to "the threat posed to the United States and Russia." With the designation, explains Benjamin, the State Department will help support U.S. efforts to reduce the group's ability to launch attacks as it tries to expel the Russian government from the North Caucasus region.[14]

An American-Somali charged for financing Al Shabaab: Ahmed Hussein Mahamud was arrested in Columbus, Ohio, on June 9th for allegedly providing money and personnel to Al Shabaab, a group listed as a terrorist organization by the U.S. State Department. The indictment alleges that Mahamud "unlawfully and knowingly" conspired with others to provide support to Al Shabaab on or about April 20, 2009 and on or about July 27, 2009 and other unknown dates. While, the indictment revealed no information on the amount of money provided or the number of people recruited by Mahamud, it alleges that he conspired with others to knowingly provide material support to be used

in Somalia by members of Al Shabaab. Court documents indicated that Mahamud is the 20th person from Minnesota believed to have returned to Somalia to join Al Shabaab since late 2007. According to a *Star Tribune* article, this trend has led to what is considered one of the largest counter-terrorism investigations since September 11, 2001. Federal officials claim that eight of the 20 charged have been arrested in the United States or overseas.[15]

Terrorism financing after the death of Usama bin Laden: According to global news reports, counter-terrorism analysts have begun assessing the impact of Usama bin Laden's death, which happened on May 2nd in Pakistan, and its impact on Al Qaida's finances. An article by *VOA News* claims that the death of Al Qaida's leader will likely have a negative impact on the group's ability to raise money and finance large-scale terrorist attacks in the future. The article quotes Stuart Levey, the former undersecretary of terrorism and financial intelligence at the U.S. Treasury Department, who described bin Laden as the "primary inspirational figure" both for recruiting new members and for the funding of the terrorist group. The director of the program on counter-terrorism and intelligence at the Washington Institute for Near East Policy, Matthew Levitt, also claims that the death of bin Laden helped create further damage to the terrorist organization and in so, fundraising will surely be affected. The article further claims that while Al Qaida receives most of its funding from wealthy donors in the Gulf, intelligence suggests that the terrorist organization has, in recent years, been struggling to raise significant amounts of money due to government efforts in those countries to counter terrorism financing. Furthermore, counter-terrorism efforts by the United States and its allies have forced Al Qaida to decentralize its fundraising activities, causing the group's affiliates to conduct their own funding operations. In a *BBC* report, Anna Murison, an analyst of the intelligence company "Exclusive Analysis", explains that with stricter terrorist financing regulations, funding for large-scale terrorist attacks has decreased and extremists will focus more on low-budget attacks. The *BBC* report also states that in addition to bin Laden's death, Al Qaida's supposed chief financial officer, Sheik Sa'id al-Masri, was also reported dead in May 2010. The report claims that with the death of these two main leaders, Al Qaida may potentially suffer financially. In a *Thomson Reuters* article, however, other counter-terrorism analysts claimed that it is too soon to know how bin Laden's death will have an impact on fundraising for Al Qaida. Dennis Lormel, the former head of the Federal Bureau of Investigation's Terrorist Financing Operations Section, states that bin Laden has been "somewhat irrelevant as a terrorist" over the past few years and, as such, there should be no major movement or changes in the flow of funds by terrorists. Nonetheless, David Cohen, the Assistant Secretary for Terrorist Financing at the U.S. Treasury Department was quoted in a *Thomson Reuters* article claiming that "the death of bin Laden is a tremendously important step and it takes away a person who at minimum, as a symbol, was helpful in raising terrorism money."[16]

FINANCIAL ACTIVITY-BASED

Suspicious activity reports lead to terrorist financing charges against two U.S. imams tied to the Pakistani Taliban: Financial institutions' suspicious activity reports (SARs) aided the Federal Bureau of Investigation (FBI) in indicting two South Florida imams and a third family member on May 14th for allegedly funnelling more than US$50,000 to the Pakistani Taliban. Hafiz Khan, imam of the Flager Mosque in Miami, and his two sons, Irfan Khan and Izhar Khan (the imam of the

Jamaat Al-Mu'mineen Mosque in Margate), were arrested in the United States while three co-defendants based in Pakistan were charged for their participation. All six defendants are accused of conspiring to provide and for providing material support to the Pakistani Taliban, a designated terrorist organization in the United States. Additionally, a U.S. Attorney claimed that Hafiz Khan allegedly built a madrassa in Pakistan's Swat Valley that provided shelter for the Pakistani Taliban and trained children to become military fighters for the mujahideen. The indictment states that, between 2008 and November 2010, the defendants provided material support by soliciting, collecting and transferring money from the United States to the Pakistani Taliban and its supporters, including the mujahideen. The indictment states that the defendants created a network for the flow of money and the amounts transferred typically ranged from US$500 to US$2990. The indictment also describes a number of occasions where Hafiz Khan transferred money to Pakistan, which was withdrawn immediately upon arrival. While the indictment does not mention the names of financial institutions that were allegedly used by the conspirators, it was the SARs submitted by various banks, combined with other evidence, that led to the terrorist financing charges. According to Dennis Lormel, the former head of the FBI's Terrorist Financing Operations Section, this specific case demonstrates how good compliance work from banks and follow-ups by law enforcement are important in identifying suspicious activity. On May 11th, the Treasury Department's Financial Crimes Enforcement Network (FinCEN) released a report stating that 711 SARs were filed by banks in 2010 that detected possible terrorist financing, which is an increase of 30% from the 545 reports filed in 2009.[17]

U.S. citizen pleads guilty to conspiracy to support "violent jihad": Zakariya Boyd, a U.S. citizen and resident of North Carolina, pleaded guilty on June 7th to one count of conspiracy to provide material support to terrorists. Boyd was originally indicted in 2009 along with seven other defendants, including his father and brother, for conspiring to support jihadist recruitment by offering money, transportation, training and other resources. According to the indictment, from before November 2006 to July 2009, the Boyds and the other defendants conspired to advance "violent jihad" which included committing acts of murder, kidnapping and maiming persons abroad. As a part of the conspiracy, the indictment states that the defendants offered aspiring terrorists training on weapons and financing, as well as arranging overseas travel and contacts to "wage violent jihad overseas." The defendants also solicited donations to support training efforts, concealed the ultimate destination of the money from the donors and obtained assault weapons to develop weaponry skills. According to the court records, the co-conspirators also radicalized others to believe that violent jihad was a religious obligation, plotted to kill U.S. military personnel by attacking a Marine Corps Base, and offered to die as martyrs. Boyd's father, Daniel P. Boyd, pleaded guilty in February 2011 to two counts of terrorism conspiracy. According to prosecutors, Zakariya Boyd could face up to 15 years in prison. Trial for the remaining co-conspirators is scheduled for September 2011.[18]

American-Lebanese couple pleads guilty to financing Hizballah: Hor and Amera Akl, both dual citizens of the United States and Lebanon, pleaded guilty on May 23rd to planning to ship up to US$1 million in the course of a year to Hizballah, an organization listed as a terrorist entity by the United States in 1997. According to assistant U.S. Attorney

Justin Herdman, investigators built the case by compiling telephone recordings and by using a Federal Bureau of Investigation (FBI) informant who provided the couple with US$200,000 for their first shipment of funds. Court documents revealed that Hor Akl travelled to Lebanon in March 2010 to arrange the delivery of the money, which was to be hidden inside an SUV, and upon his return to the United States, he claimed he had met with Hizballah officials. Herdman declared that the Akls were aiming to make a profit of about US$200,000 in fees to transfer the funds. Both Hor and Amera pleaded guilty to conspiracy to provide material support to a foreign terrorist organization. Hor also pleaded guilty to money laundering, bankruptcy fraud and perjury charges. However, according to the plea agreement, with the testimony of both defendants, the money laundering charges as well as other charges were dropped. The couple went from facing up to life in prison to now facing a sentence of a little over seven years for Hor and up to four years for Amera.[19]

Somali national sentenced for smuggling activity tied to terrorism: Ahmed Muhammed Dhakane, a Somali national who knowingly smuggled people linked to a terrorist group into the United States, received a 10-year prison sentence on April 28th. Dhakane pleaded guilty in November 2010 to making false statements on his 2008 asylum application. According to the *Investigative Project on Terrorism (IPT)*, Dhakane failed to indicate on his application his connections to two terrorist organizations, Al-Ittihad Al-Islami (AIAI) and al-Barrakat, as well as running a smuggling operation out of a hotel in Brazil where he brought members of one of those terrorist groups into the United States. According to Federal Bureau of Investigation (FBI) special agent, Mark Wagoner, while the total number of people affiliated with terrorist groups whom Dhakane smuggled into the country is unknown, Dhakane has provided the names of seven of his smuggling clients linked to the Somali-based organizations of AIAI, the Council of Islamic Courts (CIC) and Al Shabaab. According to Dhakane, he believes these individuals would "pick up arms" against the United States if the jihad moved from overseas to the country. Dhakane also admitted to an FBI informant that he was an AIAI member and that he was once a fighter for the group. The *IPT* also reports that Dhakane worked for al-Barrakat, another designated terrorist organization. According to the research group, al-Barrakat is an informal money transfer network with a militia, set up after the Somali government and the central bank collapsed in the 1990s. U.S. officials believe that al-Barrakat has ties to terrorism financing; a review of al-Barrakat's financial records by the FBI revealed a number of suspicious transactions which al-Barrakat's owner could not explain. Aside from his terrorism-linked activities, Dhakane was also involved in smuggling hundreds of individuals into the United States while he was working for a well-known smuggler based out of São Paulo. When Dhakane broke off to create his own operation, he testified in court to having smuggled between 20-50 people. Although Dhakane was not directly convicted of a terrorism crime, the court's judge ruled that Dhakane's sentence be lengthened due to the case's connection to terrorism, including harbouring terrorists and material support.[20]

COUNTRY-BASED

President of Nigeria signs terrorism, money laundering bills: On June 3rd, the President of Nigeria, Goodluck Jonathan, signed two bills into law – the *Terrorism (Prevention) Bill, 2011* and the *Money Laundering (Prohibition) Bill, 2011*. According

to a government official, the new *Terrorism (Prevention) Act, 2011*, establishes measures for the "prevention, prohibition and combating of acts of terrorism and the financing of terrorism" in Nigeria. Similarly, the Act also provides effective implementation of the Convention on the Prevention and Combating of Terrorism as well as the U.N. Convention of the Suppression of the Financing of Terrorism. Finally, the Act prescribes penalties for the violation of its provisions, including a maximum sentence of 20 years in prison. The *Money Laundering (Prohibition) Act, 2011* replaces the 2004 *Money Laundering Act* and makes "comprehensive provisions" to suppress the laundering of illegal proceeds. The Act also expands the powers of supervisory and regulatory authorities in Nigeria to address any challenges faced in implementing the anti-money laundering regime in the country.[21]

Somalia sentences Westerners over pirate ransom: On June 18th, a Somali court jailed six foreigners for illegally bringing in millions of dollars into the country to pay pirates ransom money for the release of captive vessels. Authorities seized two aircrafts carrying the ransom money of US$3.6 million in Mogadishu in late May; the cash and planes are now the property of Somalia's government. According to *Thomson Reuters*, although piracy off the Horn of Africa has increased and the practise of paying ransom money is common, the Somali government has declared it illegal to pay off armed gangs. The Mogadishu court announced in a precedent-setting case that of the six foreigners, three are British and one is American, making it the first time that Westerners are sentenced over ransom payments in Somalia. The court sentenced two pilots, who are American and British nationals, each to 15 years in prison and a US$15,000 fine. The four others, two of whom are Kenyan, were sentenced to 10 years in jail and a US$10,000 fine each. The court's judge added that all six can appeal their jail sentence by paying more money. According to *Thomson Reuters*, cash ransoms are usually dropped onto captured vessels from light aircraft. Maritime piracy costs the global economy up to US$12 billion annually.[22]

BIBLIOGRAPHY

1. Myers, Laura L. “Colombian FARC narco-terrorists convicted in Seattle.” *Thomson Reuters.* May 4, 2011.

2. "Police smash major drug ring operating 'super labs' after man reported missing." *Canadian Press*. May 25, 2011.

Chen, Dalson. "Women arrested in ecstasy bust." *Windsor Star*. May 12, 2011.

Sher, Julian. "Drug trafficking/World Drug Report 2011." *Globe and Mail.* June 24, 2011.

3. Denis, Lessard. “Attention, fraudeurs.” *La Presse*. April 27, 2011.

4. Hundley, Kris. “Online poker investors lose big as rules change.” *St. Petersburg Times*. May 1, 2011

Lord, Simon. “Full Tilt Poker bloqué.” *Le Journal de Montréal.* June 30, 2011.

Monroe, Brian. “Justice Department Seeks $3 Billion from Online Gambling Companies that Used Complicit Banks.” *Moneylaundering.com*. April 15, 2011.

United States Department of Justice. “Manhattan U.S. Attorney charges principals of three largest Internet poker companies with bank fraud, illegal gambling offenses and laundering billion in illegal gambling proceeds.” *Press release.* United States of America. April 15, 2011.

Williams, Adams. “After U.S. crackdown, online poker headquarters raided in Costa Rica.” *Ticotimes.* May 8, 2011.

Wolf, Brett. “Justice Department targets online gambling firms and payment processors.” *Thomson Reuters*. April 15, 2011.

5. “Cyber thieves hacking U.S. small firms sending money to China.” *Bloomberg*. April 27, 2011.

6. Hermann, Peter. “Lottery used to launder drug money, federal authorities say.” *Baltimore Sun*. April 28, 2011.

Torbati, Yeganeh June. “Prosecutors: Alleged drug dealer laundered money via Md. Lottery.” *Baltimore Sun*. April 27, 2011.

United States Department of Justice. “Superseding Indictment charges Steven Blackwell and Joy Edison in $10 million heroin and money laundering conspiracy.” Press release. United States of America. April 27, 2011.

7. “East Bay Woman Indicted for Running Student Visa Scam.” *KTVU.com*. May 3, 2011.

Lisa. “Tri Valley University president arrested by federal agents.” *Visablog.com*. May 13, 2011.

United States of America v. Poul Thorsen. Criminal Indictment No. 1: 11-CR-194. *United States District Court.* April 13, 2011.

Wolf, Brett. “Danish doctor stole and laundered CDC funds, prosecutors say.” *Thomson Reuters*. April 14, 2011.

Wolf, Brett. “University president in California laundered visa fraud proceeds, persecutors say.” *Thomson Reuters*. May 4, 2011.

8. Adams, Colby. “Loosely managed digital currency couldn’t be avenue for crime that’s hard to block”. *Moneylaundering.com*. April 15, 2011.

Ball, James. “Bitcoins: What are they, and how do they work?” *Guardian*. June 22, 2011.

Ball, James. “LulzSec rogue suspected of Bitcoin hack.” *Guardian*. June 22, 2011.

Basulto, Dominic. “What happens when anonymous gets a bank?” *Bigthink.com*. May 18, 2011.

Brito, Jerry. “Online cash Bitcoin could challenge governments, Banks.” *Time Inc*. April 6, 2011.

Reitman, Rainey. “Bitcoin, A step toward censorship resistant digital currency.” *Electronic frontier foundation*. January 20, 2011.

Schwartz, Mathew J. “LulzSec hackers using digital currency: DEA crackdown soon?” *InformationWeek*. June 28, 2011.

Wolf, Brett. “US Senators ask DoJ target online currency known as ‘Bitcoins’.” *Thomson Reuters*. June 7, 2011.

Wolf, Brett. “Senators’ criticism prompts ‘Bitcoin’ exchanges to offer cooperation against laundrymen.” *Thomson Reuters*. June 15, 2011.

Wolf, Brett. “Senators seek crackdown on “Bitcoin” currency.” *Thomson Reuters*. June 8, 2011.

9. “Mexico set rewards for reporting money laundering.” *Associated Press*. April 4, 2011.

Wolf, Brett. “Mexico sets money-laundering whistleblower program.” *Thomson Reuters.* April 6, 2011.

10. “Improving Global AML/CFT Compliance: on-going process - 24 June 2011.” *Financial Action Task Force.* June 24, 2011. Web.

“Outcomes of the Joint Plenary meeting of the FATF and GAFISUD, Mexico City, 22-24 June 2011” *Financial Action Task Force.* Paris: June 27, 2011. Web.

Bronstein, Hugh. “Argentine money laundering bill passes Senate.” *Thomson Reuters*. June 1, 2011.

11. Global Press Service. “Eight ways to transfer illegal assets overseas.” *Thomson Reuters*. June 16, 2011.

12. Tampubolon, Hans Davis. “Money laundering probe starts at Citibank.” *Jakarta Post*. June 21, 2011.

Vagen, Trond. “$2m theft puts Citibank in AML spotlight in Indonesia.” *Thomson Reuters*. April 27, 2011.

13. Blumberg, Mark. "Canadian Charities Recently Revoked by the Charities Directorate of CRA for Cause 2011." *Blumbergs*. April 23, 2010.

Canada Revenue Agency. “Re: Audit of World Islamic Call Society.” Letter. Government of Canada. October 4, 2010.

Dimmock, Gary. “Gadhafi Charity in Canada linked to terrorism.” *Ottawa Citizen*. May 7, 2011.

14. Crawford, Jamie. “U.S. designates Chechen group in North Caucasus as terrorist entity.” *CNN*. May 27, 2011.

15. United States Department of Justice. “Ohio man charged with providing material support to terrorist group based in Somalia.” Press release. United States of America. June 9, 2011.

Walsh, James. “Somalis facing terror charges now number 20.” *StarTribune*. June 9, 2011.

16. Buel, Meredith. "Experts: Bin Laden' death has negative impact on financing." *VOANews.com*, May 5, 2011.

Global Press Service. "Bin Laden death may limit terror financing." *Thomson Reuters*. May 4, 2011.

Melik, James. "Funding terrorism: Tracking resources remains a priority." *BBC News.* May 4, 2011.

Wolf, Brett. "Too early to know how bin Laden's death will affect Al Qaeda's finances, say experts." *Thomson Reuters*. May 2, 2011.

17. "North Carolina man pleads guilty to terrorism conspiracy." *CNN*. June 15, 2011.

Federal Bureau of Investigation. "North Carolina man pleads guilty to terrorism charge." Press release. United States of America. June 7, 2011.

Wolf, Brett. "SARs lead to terrorist financing charges against South Florida imams." *Thomson Reuters.* May 14, 2011.

18. Seewer, John. "Ohio couple pleads guilty in terror funding case." *Associated Press*. May 23, 2011.

19. "Somali Human Smuggler Sentenced to 10 years." *Investigative Project on Terrorism News*. April 29, 2011.

20. Ailemen, Tony. "Nigeria: Jonathan Signs Terrorism Bill." *Daily Champion*. June 7, 2011.

Akintola, Kehinde. "Senate passes Anti-Terrorism Bill." *Business Day.* February 18, 2011.

Archibong, Elizabeth. "Jonathan signs terrorism, money laundering bills." *Next*. June 7, 2011.

21. "U.S. imams arrested for aiding Taliban." *Thomson Reuters*. May 15, 2011.

"U.S. imams arrested for alleged Pakistani Taliban links." *CNN*. May 16, 2011.

Wolf, Brett. "SARs lead to terrorist financing charges against South Florida imams." *Thomson Reuters.* May 14, 2011.

22. "Somalia jails Britons, American over pirate cash." *Emirates 24/7*. June 19, 2011.

Ahmed, Mohamed. "Somalia jails Britons, American over pirate ransom." *News Daily*. June 19, 2001.