MONEY LAUNDERING
AND TERRORIST ACTIVITY FINANCING WATCH

January-March 2010

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 and terrorist activity financing issues;
- Alerts readers to new developments that could possibly be exploited for money laundering or terrorist activity financing purposes in Canada.

ML/TF Watch *is a quarterly review of news articles and is compiled by FINTRAC's Macro-Analysis and Research unit. It provides links to more detailed information sources (all references mentioned are hyperlinked to their sources). The articles provided in this issue range from January 2010 to March 2010.*

Caveat

The views expressed herein are those of the original authors except where specifically noted.

Money Laundering

Terrorist Activity Financing

Money Laundering

GROUP-BASED

Italian mafia launders money through telecom companies: One of the biggest fraud cases in Italian history has recently surfaced, and allegedly involves 'Ndrangheta (the Calabrian mafia), telecom broadband operators Fastweb and Telecom Italia Sparkle (TIS), as well as an Italian politician. On February 23, the release of 1,600 pages of court documents outlined the arrest warrants of 56 people in Italy, the United States, the United Kingdom and Luxembourg. These individuals were all suspected of being involved in a scheme that facilitated tax evasion and money laundering, as well as "breaking electoral laws with mafia involvement." According to court documents, Fastweb and TIS were complicit in a tax evasion scam and money laundering scheme that generated a total of €2.2 billion in profit between 2003 and 2007, and allowed the fraud participants to collect more than €300 million in Value Added Tax (VAT) credit. Prosecutors have additionally charged TIS with "administrative responsibility in relation to international criminal organization and money laundering."

The case is still under investigation and many details of the scheme remain to be explained by officials. Nonetheless, the investigation did uncover evidence that linked one of the masterminds of the telecommunications fraud, Gannaro Mokbel, with a 2008 election that was rigged by the Calabrian mafia. 'Ndrangheta, acting at the request of Mokbel, allegedly sent some of its group members to Germany to buy thousands of blank voting ballot sheets for Nicola Di Girolamo, Mokbel's friend. Di Girolamo, who was also one of the 56 arrested, was elected as a senator for Italian Prime Minister Silvio Berlusconi's party. In return for 'Ndrangheta's help, Mokbel instructed Di Girolamo to assist the mafia in laundering its profits from Europe's cocaine trade.[1]

FINANCIAL ACTIVITY-BASED

ML through online gambling: On March 25, Michael Olaf Schuett pleaded guilty to operating an unlicensed money transmitting business in the United States that received wire transfers from Internet gaming companies in Europe. Since November 2007, Schuett, a German national who was in the United States on a tourist visa, transferred US$ 70 million in online gaming winnings to 23,000 people, primarily living in the United States. Court documents indicate that Schuett controlled 424 Florida shell corporations that were registered under his home address in Florida. Of those companies, nine were used to conduct unlicensed money transfers. The companies held accounts at banks, including: Ironstone, SunTrust, Regions Bank, BB&T, Iberia Bank, and the Bank of America—where Schuett had opened 40 accounts alone. Wire transfers that were sent to Schuett came mainly from the British-based company Bluetool Ltd. and the German-based company International Payment Systems. Upon receipt of the funds from accounts overseas, Schuett obtained large numbers of cashier's cheques, wrote business cheques, and sent wire transfers to game winners in the United States and Canada. Officials believe that Bluetool and International Payment Systems are being used by online gaming companies as intermediaries to transfer funds to U.S.-based money transmitters in order to disperse gaming winnings to U.S.-based customers. At the time of this article's publication, federal agents sought to seize Schuett's computers, a Powership Federal Express shipping device,

several luxury items and the funds in nine bank accounts held by Schuett's companies: MI Global, MCM Capital Management, US AG 24, South Naples Escrow Company, Southwest Florida Payroll, Woodhouse Systems, Mathews Trade Corporation, South Florida Payroll and Internet Payment Services Group.[2]

Wachovia settlement over Mexican exchange houses linked to New Zealand shell companies: On March 17, Wachovia bank settled money laundering charges in the United States, by paying a US$160 million fine. The penalty addresses the bank's insufficient inspection of more than US$420 billion in transactions from Mexican money exchange houses, or *casas de cambio.* The settlement is the highest monetary penalty imposed under the *Bank Secrecy Act* and includes a US$110 million forfeiture and a US$50 million fine. The penalty is the result of a Drug Enforcement Administration (DEA) investigation which began in 2005, that uncovered a US$13 million transfer from Mexican exchange houses to the Wachovia branch in Miami for the purchase of airplanes to be used for cocaine shipments. Since then, many other U.S. government agencies have tracked billions of dollars in suspicious transactions from Mexico to Wachovia. These transactions included multiple rounded sum wire transfers to a single account on the same day, bulk cash transactions up to 50% more than what a customer had led Wachovia to expect and the deposit of traveller's cheques with sequential numbers that had unusual markings. Wachovia ended its relationship as a "correspondent bank" with Mexican exchange houses in 2008 when it was acquired by Wells Fargo as a result of the economic downturn.

Concerns regarding Wachovia's transaction monitoring practices were also raised in 2006 when a compliance officer at a U.K. Wachovia branch observed improperly endorsed, sequentially numbered and large denomination cheques from Mexican exchange houses. The suspicious activity was reported to the Serious Organized Crime Agency (SOCA) in the United Kingdom. However, according to a lawsuit filed by compliance officer Martin Woods, Wachovia executives dismissed his scrutiny of the Mexican exchange houses and bullied and demoted him. He also noticed that within months of reporting the suspicious activity to SOCA, the Mexican exchange houses stopped routing traveler's cheques through London. A Wachovia spokesperson claims that no evidence was found to suspect that staff members tipped off the Mexican exchange houses' clients about Woods' suspicions. Nevertheless, within a year of the reporting, the DEA raided the office of one of the suspicious Mexican exchange houses, Casa de Cambio Puebla, and discovered evidence that it had been used by the Sinaloa drug cartel to purchase two airplanes for the transportation of US$1 billion worth of cocaine. In May 2007, the DEA froze Puebla's Wachovia bank accounts held in Miami and London. Furthermore, Mexican authorities closed down the exchange house and arrested its executive, Pedro Alatorre Damy, who was allegedly the "financial mastermind" of the Sinaloa cartel.

The Wachovia settlement has links to various other money laundering and terrorist financing activities, including the exploitation of New Zealand's weak company registration laws and weapons trafficking from North Korea. In New Zealand, four firms (Keronol Ltd., Melide Ltd., Tormex Ltd., and Dorio Ltd.) are alleged to have laundered Mexican drug proceeds from the Sinaloa cartel using Latvian bank accounts and Wachovia's London branch. The four firms, which all had bank accounts in Latvia, transferred approximately US$40 million from their respective accounts

to Wachovia in London. In addition, the Sinaloa cartel funnelled money to the Latvian bank accounts through Wachovia, via the Mexican exchange houses. The four New Zealand firms were all found to be registered at 369 Queen St., 5th Floor, Auckland, New Zealand along with 338 other companies. Results of the investigation of these activities highlights "potentially dangerous gaps" in New Zealand's company registration system which could enable shell companies to launder money for criminals, drug cartels, and/or terrorist financiers. According to the Financial Action Task Force (FATF), New Zealand has many gaps in its money laundering laws that it has not yet addressed, such as not having a legal requirement for financial institutions to identify the beneficial owner of companies.

Additionally, some of the funds from the Mexican exchange houses that passed through Wachovia's London office have been linked to the seizure of a plane smuggling arms from North Korea to Iran. On December 12, 2009, a plane carrying 35 tons of explosives and anti-aircraft missiles from North Korea bound for Iran was seized by police in Bangkok. The plane was leased by SP Trading Ltd, a company which was registered under the same New Zealand address as the four firms implicated in laundering Mexican drug money. Furthermore, the companies that conducted the Wachovia wire transfers and SP Trading Ltd. were owned by VicAm (Auckland) Ltd. VicAm is a New Zealand corporation owned by GT Group, a consulting company that provides financial secrecy by selling shell companies to others while keeping their identities secret. According to *Complinet,* VicAm is the sole shareholder of 1089 New Zealand companies.[3]

FIFA to tackle money laundering in football: FIFA, the international organization governing the sport of football (soccer), plans to introduce a mandatory international transfer system of players to reduce money laundering and fraud in the sport. According to Mark Goddard, general manager of the new system, the current lack of "significant oversight or regulation" makes the sport appealing to money launderers, who, for instance, make payments to fictitious players in order to launder their funds. Every year, between 20,000 and 30,000 cross-border deals worth approximately US$1 billion take place in the football sector. The sector is not strictly regulated and the transfer of players is not subject to rigorous oversight. The new Transfer Matching System will require clubs to record information such as player identities, contract information, and total agent payments and fees in order to enable auditors to inspect international deals. The Transfer Matching System will help regulate the football transfer market, and is also expected to reduce the amount of unfair deals involving agents who recruit talented young players from areas such as South America. [4]

ML through free trade zones: According to a recent report published by the FATF, free trade zones may not be keeping up-to-date with anti-money laundering standards. These zones, which require less stringent inspection of goods and are subject to less thorough record keeping obligations than standard ports, are described as posing "huge vulnerabilities". They are used by organized crime organizations in China, Russia and Bahrain. According to FATF, goods that are often exploited by the lax safeguards surrounding free trade zone tend to be items that are easy to repackage or reship, such as cigarettes, alcohol and luxury items. Free trade zones are often vulnerable to trade-based money laundering techniques such as under-and over-pricing goods. FATF also

indicates that the matter of identifying suspicious transactions involving free trade zones is made difficult by the fact that certain jurisdictions do not require companies active in the free trade zones to report high-value currency transactions or suspicious activity. FATF notes that certain indicators can assist banks to investigate accounts for suspicious activity related to free trade zones. These indicators include: "free trade transactions involving seemingly unrelated third parties, repeatedly extended letters of credit and the use of fiduciary companies established in the zones." Companies which have a high volume of business but low capitalization are also of concern. Today, there are approximately 3,000 free trade zones in 135 countries with exports valued at a total of US$400 billion, according to data from 2007. The most significant trading in free trade zones is conducted in China, Panama, and the Middle East.[5]

Western Union pays US$94 million to settle lawsuit tied to ML and human smuggling: After four years, on February 11, Arizona's Attorney General's Office succeeded in gaining Western Union's cooperation with investigations related to human smuggling activity from Mexico. Western Union acknowledged that, between 2003 and 2007, certain agents at several of its locations were engaged in laundering money. The company agreed to pay a US$94 million settlement. In 2006, Arizona state examiners uncovered numerous anti-money laundering (AML) compliance violations by Western Union that were tied to cash and human smuggling. According to court documents, transactions used to pay smugglers to bring "illegal immigrants across the Arizona-Mexico border" were uncovered. The company processed more than US$176 million in remittances sent from 29 states that are known to be frequent destinations for persons being smuggled from Mexico. The money was sent to eight Western Union locations in Arizona. As part of the agreement, Western Union is required to pay US$23 million to improve its AML program, US$21 million to Arizona, and US$50 million to a non-profit organization that will distribute the funds to law-enforcement agencies that conduct investigations along the U.S.-Mexico border. Furthermore, Western Union has agreed to provide information to human smuggling and trafficking investigators in Arizona, California, New Mexico, and Texas.[6]

Use of 'factoring' to launder money grows in Latin America: Loan service businesses may increasingly be used by money launderers to introduce dirty money into the legitimate economy, according to *moneylaundering.com*. One of the impacts of the global recession has been a decrease in the amount of credit offered by banks, and an increased difficulty to cover business operating costs. As a result, some businesses are selling their accounts receivable at discounted prices to invoice finance companies, also called "factors". The exercise of factoring by money launderers is reportedly increasing in South America, and is mostly prevalent in the layering and integration stages. Two ways factoring companies can be used to launder money include payments against invoices for products that have not actually been sent to the buyer, and inflating the value of the goods in order to overvalue the invoice. The factoring company may be a knowing participant in the money laundering scheme. For example, it can work in tandem with the company selling invoices to launder money; or it can be an unwitting participant, for instance when the company selling the invoices collaborates with the buyer of the goods or services to launder money through the factoring company. According to Factors Chain International, the industry group's network, the factoring turnover in Argentina, Brazil, Chile, Colombia and Mexico doubled between 2004 and 2008 from US$32 billion to

almost US$65 billion. According to FinCEN, financing companies are not subject to any "special AML regulations".[7]

IMF launches program to help African countries counter ML/TF through precious metals: The International Monetary Fund (IMF) will provide 16 sub-Saharan African countries with technical training to help counter money laundering and terrorist financing in their diamond and gold markets, the latter contributing US$25 billion annually to the global economy. According to the U.S. State Department's Kimberley Process Authority, concerns regarding the use of gold and diamonds to launder money internationally are not surprising, considering there is a lack of security in the region and there are no anti-money laundering practices governing the precious metals industry in Africa. Additionally, financial institutions and other companies find it challenging to perform due diligence since secrecy laws (often linked to the mining industry) make it difficult to confirm all parties involved in transactions related to precious metals. Another programme that helps prevent corrupt payments in the industry is led by a Norwegian-based lobby group, Extractive Industries Transparency Initiative (EITI) that requires companies and governments to disclose what they pay or receive for mining contracts. There are 32 countries that have agreed to implement EITI standards, of which 19 are in Africa. According to EITI, international financial institutions should ensure that countries and businesses are EITI compliant before conducting business or delivering aid.[8]

COUNTRY-BASED

FinCEN broadens law to allow foreign law officials data requests: The U.S. Treasury Department implemented new rules on February 5 that expand the types of law enforcement data requests U.S. banks can receive. The rule expands the *U.S. Patriot Act* Section 314 (a) which previously only allowed requests applied to investigations of alleged terrorist financing and money laundering. Now, foreign law enforcement agencies are able to send requests concerning cases of suspected fraud, drug trafficking and other crimes to U.S. financial institutions, which then have two weeks to respond with data. FinCEN, which will also be allowed to issue requests under section 314 (a) to U.S. financial institutions, estimates that the new rule will add 72 hours of compliance work annually to each bank. Financial institutions however, are concerned that the compliance burden will increase beyond this moderate estimate. FinCEN further stated that it would only respond and release information to countries which the United States has a mutual legal assistance treaty and which supply similar data to the United States. Additionally, a request received by a U.S. financial institution will only require it to acknowledge if matching transactions or accounts exist; additional information about the transactions and/or accounts will have to be obtained via subpoena. According to FinCEN's 2009 Annual Report, there have been 1,061 requests from 24 federal agencies, resulting in nearly 67,500 total matches, since November 2002.[9]

Gap in U.S. regulations over MSBs' and casinos' sanctions compliance: According to James Dowling, former special agent with the Internal Revenue Service (IRS), the IRS does not have the mandate to assess possible sanctions violations or enforce rules on how

money service businesses (MSBs) and casinos comply with economic sanctions. AML examiners at the IRS can note whether an MSB is compliant or non-compliant with economic sanctions but the IRS does not have the authority to force MSBs or casinos to set up a sanctions program. This "lack of clear regulatory oversight" results in inadequate supervision of sanctions compliance imposed by the Office of Foreign Assets Control (OFAC) and the U.S. Justice Department. As such, economic sanctions may be evaded when dealing with an MSB or casino that has a weak sanctions monitoring program. In 2006, the IRS and OFAC began working together on an initiative that would allow IRS examiners to ask questions regarding OFAC compliance standards during *Bank Secrecy Act* examinations. However, the initiative is not as uniformly enforced as it was originally intended. In some states, such as New York, Texas and Florida, IRS examiners are known for stressing OFAC programs in their examinations of MSBs by testing the companies filtering software. In other regions however, some IRS and state examiners simply ask if the MSB knows of OFAC and whether they have a sanctions filtering system in place. According to *moneylaundering.com*, if a U.S. casino does not have a proper filtering system, OFAC sanctions could be violated should a U.S.-blacklisted individual transfer money from a foreign casino to one in the United States, thus going outside "standard financial transfer routes" to send money. [10]

New 'Trade Transparency Unit' in Panama: In 2010, Panama will become the seventh member of the 'Trade Transparency Unit' (TTU) network, a U.S.-led initiative designed to promote information sharing between member countries to detect trade-based money laundering. The program allows participating countries to see both sides of import and export transactions for goods that enter or exit their borders. Trade-based money laundering is often difficult to detect. Customs officials are often unable to observe the monetary transactions related to the goods, while reporting entities such as financial institutions may have difficulty in ascertaining the value of the goods involved in the transactions because they only see paperwork rather than the goods themselves. TTUs were initially created in the 1990s by the United States, which was concerned about the misuse of trade between Colombia and the United States to launder drug proceeds. Currently, the four other members of this network are: Brazil, Paraguay, Argentina and Mexico. [11]

PayPal suspends personal payments in India: On February 8, PayPal operations in India were suspended until March 3 due to a lack of authorization from the Reserve Bank of India (RBI) needed to provide cross-border money transfers. All personal payments to and from India were suspended and while customers were still able to make commercial payments to India, local merchants could not withdraw funds from banks. According to a spokeswoman for the RBI, India's *Payments and Settlements Systems Act* states that no person other than the RBI can operate a payment system, unless it has been authorized within six months of the commencement of the Act in August 2008. As of January 31, Western Union and MoneyGram were some of the payment systems authorized to conduct cross-border money transfer into India. The Indian government is concerned that intermediary money payment systems such as PayPal are being used by freelance writers and software developers attempting to evade taxes for income earned abroad and by terrorist financiers in India. PayPal may be required to tighten its verification of user accounts in India to meet the new rules introduced last November aimed at preventing money

laundering. However, PayPal's user agreement states that it cannot guarantee user identity because "user verification online is difficult".

On March 3, PayPal received authorization from the RBI to resume bank withdrawals for settlements relating to the exports of goods and services, but personal payments remain suspended. Henceforward, PayPal users will be required under Indian laws to submit a "Purpose Code" that specifies the nature of the cross-border transaction. PayPal in India can no longer be used to process charitable payments or donations and is still waiting for specific government approval to allow Personal Inward Remittance to India.[12]

Report deems Ecuador to be emerging 'hub' for international crime: A 77-page report released by the International Assessment and Strategy Center (IASC) on January 24 reveals weaknesses and concerns regarding Ecuador as a "hub" for international crime. According to the report, Ecuador's lax regulations allow approximately US$500 million to US$1 billion to be laundered through its financial system annually. Transnational criminal organizations from Latin America, Russia, China, India, and Africa are able to conduct business in Ecuador due to its weak institutions and AML laws, non-existent counter-terror financing (CTF) laws, as well as the infiltration of Ecuador's government and judiciary by the Revolutionary Army of Columbia's (FARC), and the country's "porous" borders. The report states that Ecuador is a prime location for international criminals to operate because of the adoption of the U.S. dollar as Ecuador's national currency in 2002, the lifting of visa requirements in 2008 and its strong bank secrecy laws. These factors enable Russian criminal organizations to sell weapons to FARC and launder money for Mexican drug smugglers, as well as for Asian and African human smugglers. The report further reveals that Ecuadorian government investigations found evidence that linked the FARC to an extensive network in Ecuador. The details also showed a link between one of President Rafael Correa's closest aids and the FARC, claiming that the designated terrorist organization may have partially funded Correa's 2006 election campaign. Finally, an agreement between Ecuador's central bank and the Export Development Bank of Iran (EDBI) to deposit US$120 million in Ecuador for trade purposes increased suspicion regarding Ecuador's financial dealings. The agreement, concluded a month after the U.S. treasury department imposed sanctions on EBDI, also allows Iran's Bank Saderat (an EBDI subsidiary) to open a branch in Ecuador.

In 2007, Ecuador was warned by the Financial Action Task Force (FATF) that it failed to comply with 48 of its 49 recommendations. On February 18, 2010, the FATF placed Ecuador on a blacklist of jurisdictions that have "strategic deficiencies" in their AML/CTF standards. Others on the list include Iran, North Korea, Ethiopia, Angola, Pakistan, Turkmenistan, São Tomé, and Príncipe. In response to the classification, Ecuador has attempted to address some of the FATF's concerns, such as criminalizing money laundering and improving procedures for freezing and seizing illegal assets. The government has also pledged to battle corruption and provide more training in detecting and combating money laundering.[13]

Report on doing business in Russia reveals "grey practices": A report written by The Control Risks**,** an independent risk consultancy, has exposed certain practices in Russia as potential money laundering risks. The report lists issues that firms face when conducting business in Russia, such as: beneficial ownership, corrupt court systems, one-day companies, black cash,

"obnalichivanie", and non-compliant banks. More specifically, the so-called "one-day companies" are created by a company formation agent who provides ready-made pre-licensed entities for individuals seeking to avoid bureaucratic complexities in starting a company. These one-day companies actually last up to a year and are usually registered with hundreds of other companies at "mass registration addresses" which can be used to exploit legal loopholes. Black cash, according to the report, is money transacted outside of the formal financial system without being recorded. In Russia, black cash is mainly used to pay salaries and other expenses while avoiding formal records of the transaction, which leads to significant disparity between the records and the company's true finances.. Obnalichivanie is a common practice in Russia that allows companies to withdraw cash from regulated bank accounts and "generate black cash to pay for services that would otherwise be taxed". The scheme basically involves Company A employing intangible services (such as consulting) of one-day Company B. Based on false invoices, Company A pays for one-day Company B's fictitious services. Company B withdraws the funds in cash from a bank and takes a percentage for itself and the complicit bank employee. One-day Company B then gives the remainder of the cash to Company A which it uses to top up salaries and pay for other things "off the books". Finally, the report states that banks in Russia cannot be relied upon to conduct know-your-customers checks and often turn "a blind-eye" to the origin of the funds. Although Russia has made recent efforts to combat crime in the country, money laundering still remains prevalent because of, but not limited to, these grey practices.[14]

Terrorist Activity Financing

GROUP-BASED

Canada designates Al Shabaab: On March 7, the Canadian federal government formally designated Al Shabaab as a terrorist group, enabling the Crown to seize any money and assets in Canada belonging to the group. The designation would also make it easier to launch prosecutions against local operatives and recruiters. The Al Qaida affiliated terrorist group operates mostly in East Africa and leads an Islamist insurgency in Somalia. Al Shabaab, which literally translates to "the youth", uses the Internet to recruit young individuals from abroad and applies "draconian" punishments to "alleged infidels" in Somalia. Several recent cases have surfaced of young Somali men in Toronto, Canada, travelling to East Africa to allegedly join Al Shabaab fighters. Shutting down Al Shabaab operations in Somalia has proven difficult due to the country's dysfunctional government.[15]

Namouh sentenced for life term in prison under Canadian anti-terrorism law: Saïd Namouh, resident of Québec, became the first person in Québec, and second person in Canada, to be convicted under the Canadian Anti-Terrorism Act. In a February 17 decision, Namouh was declared guilty of conspiracy to detonate an explosive device, participating in a terrorist act, facilitating such an act and committing extortion for a terrorist group. He conspired to launch a car bomb attack in Vienna, Austria and was also actively involved in preparing promotional and ransom videos on behalf of the Global Islamic Media Front, an Al Qaida propaganda organization. When Namouh was apprehended, he was allegedly preparing to leave Canada in order to meet up with co-conspirers in the Maghreb region of North Africa as well as in Egypt.[16]

OFAC imposes further designations on Iran's IRGC: The U.S. Treasury Department has designated General Rostam Qasemi and four companies affiliated with the Islamic Revolutionary Guard Corps (IRGC) under Executive Order (E.O.) 13382. The order freezes the assets of designated proliferators of weapons of mass destruction and their supporters. The action focuses on Khatam al-Anbiya Construction Headquarters, which is the engineering arm of the IRGC and helps generate funds for the IRGC's operations. Qasemi is the commander of the Khatam al-Anbiya, which is involved in the construction of streets, highways, tunnels and various other construction projects. Four companies, which are either owned, controlled by, or that act on behalf of Khatam al-Anbiya were also targeted: Fater Engineering Institute, Imensazen Consultant Engineers Institute (ICEI), Makin Institute, and Rahab Institute. The IRGC has extensive economic interest in construction, defence production and oil industries, generating billions of dollars through its business. According to the U.S. Treasury, the profits from these activities allow the IRGC to finance a full range of activities, including WMD proliferation and terrorism support. The European Union has also designated Khatam al-Anbiya for its support to Iran's ballistic missile and nuclear programs.[17]

FINANCIAL ACTIVITY-BASED

Auto theft in Canada financing terrorism: According to Rick Dubin, vice-president of the Insurance Bureau of Canada, stolen cars in Canada may be financing terrorist groups abroad. Investigators have reportedly traced vehicles stolen in Canada to destinations such as Nigeria, Lebanon and Eastern Europe. According to the Bureau, high-end vehicles are the ones most targeted for theft in Canada. Dubin claims that these vehicles, although harder to steal, bring in a "strong profit", either through the sale of the car parts or through the sale of the vehicle itself. To conceal the original source of the car, crime groups may change its vehicle identification number. In a list of the top ten most frequently stolen cars in 2009, the Bureau included four models of the Cadillac Escalade SUV, and models from the Hummer, Audi and Mitsubishi brands. Similarly, the Toronto Star reported in December 2009 that auto theft, especially stolen luxury vehicles, are being shipped to and sold in the Middle East, Africa, and Eastern Europe. In some cases, the sales of stolen luxury vehicles generate funds for gangs or terrorist groups, such as Hizballah. In addition, FBI findings indicate that some vehicles stolen from the U.S. were later used in car-bomb attacks in Iraq. [18]

Four men indicted by New York prosecutors for sending money to Iran: Two separate cases that emerged in January show how hawalas are being used to send money to Iran. On January 12, Mahmoud Reza Banki, a management consultant for Manhattan McKinsey & Co, was indicted for operating an unlicensed money transmitting business that moved roughly US$ 4.7 million between the United States and Iran. From January 2006 to September 2009, Iranian expatriates residing in the United States wired money from U.S. accounts held by entities in Saudi Arabia, Kuwait, Latvia, Slovenia, Russia, Sweden, the Philippines and elsewhere to Banki's personal account that he maintained at the Bank of America in Manhattan. Once the funds were in his personal account, Banki was alleged to have asked an Iranian-based accomplice to distribute the equivalent funds, minus transaction fees, to the intended recipients in Iran. Banki was therefore alleged to be acting as an hawaladar. Banki allegedly used the funds transferred into his bank account to make joint investments in the United States with his Iranian-based accomplice.

In a separate case, on January 20, three New York men were charged for sending approximately US$300,000 to Iran and other countries via unregistered hawalas. According to two complaints, Reza Safarha, Nick Mohamey, and Mohammed Saroush separately arranged to transfer funds which were the proceeds of a computer heist. Safarha and Mohamy asked an informant to wire the funds into accounts at JP Mogran Chase and California National Bank. The money was then to be wired to Dubai and further transferred to Iran. Both cases illustrate how the unregulated money service businesses may be used to evade sanctions.[19]

Electronics and video game exports allegedly financing Hizballah: On February 19, four men and three businesses were indicted in Miami for illegally exporting electronics and video games to a blacklisted shopping center in South America that U.S. official's claim funnels money to Hizballah. According to the indictment, Khaled Safadi and Ulises Talavera-Campos of Miami and Emilio Jacinto Gonzalez-Neira and Samer Mehdi of Paraguay ran companies that used the Port of Miami to transport goods to Galeria Page Mall, a shopping centre in Ciudad del Este, Paraguay. The three companies: Transamerica Express of Miami Inc. owned by Talavera; Cedar Distributors Inc. owned by Safadi; and Jumbo Cargo Inc. owned by Gonzalez-Neira; are all freight forwarding companies based in Miami. From March 2007 to January 2008, U.S. officials claim that nearly US$1 million in exports were sent from Transamerica and Jumbo, including goods such as Sony Playstation video game consoles, digital cameras and other electronic items. The men allegedly used false invoices, addresses, and names to hide the true destination of the goods. The intended recipient was Jomana Import Export, an electronics business owned by Mehdi and located in the shopping center. Additionally, Mehdi attempted to conceal the origins of wire transfer payments to a Sony electronics distributor in Ohio by wiring the funds from a currency exchange in South America to bank accounts in New Jersey, while giving instructions to forward the money to the distributor. Galeria Page Mall was designated by the U.S. Treasury Department in December 2006 along with its owner, Muhammed Yusif Abdallah, a senior Hizballah leader in South America.[20]

COUNTRY-BASED

Manhattan's US Attorney creates the Terrorism and International Narcotics Unit: In the United States, a new unit designed to prevent extremist Islamic groups from obtaining funds from the illegal trade of narcotics has been created. The Terrorism and International Narcotics Unit is comprised of prosecutors from the US Attorney's Office in Manhattan who are experienced in dealing with terrorism and international drug issues, as well as experienced in working overseas on complex cases. The *New York Times* reports that the creation of this new unit is a reflection of the legitimate risk posed by a working relationship between terrorist groups and drug trafficking organizations. Specifically, as law enforcement scrutiny has decreased the amount of funds that terrorist organizations obtain through traditional means, terrorist groups are turning to narcotics traffickers for new sources of funds. The Terrorism and International Narcotics Unit is deemed to be the first of its kind in the United States. [21]

U.K. lawmakers to banish the freezing of funds for suspected terrorists: On January 27, Britain's Supreme Court ruled to disallow the freezing of funds belonging to suspected terrorist financiers under UN sanctions. The ruling is a part of a case review

of five men, Mohammed Jabar Ahmed, Mohammed Azmir Khan, Michael Marteen, Hani El Sayed Sabaei Youssef and Mohammed al-Ghabra, who were first sanctioned by the UN, and later appealed the freezing of their funds in the United Kingdom. Her Majesty's Treasury found it to "too severe" to block funds linked to suspected terrorists in the way mandated by UN sanctions and that such an order "profoundly" interferes with the suspects' lives. It also violates human rights because designated individuals cannot challenge UN sanctions. The U.K. ruling, which affects more than 40 people and nearly £150,000 in frozen funds, has other U.K. officials and lawmakers working quickly to pass legislation that will reverse the Supreme Court's decision. The legislation would address the court's concerns by ensuring more transparency in sanctions designations, setting higher standards for evidence, and requiring U.K. lawmakers to help determine the validity of asset freezes. The U.K. Treasury stated that it was also introducing a "fast-track legislation" to guarantee no disruption in the country's asset freezing powers. The suspects' funds will remain frozen while lawmakers work to address the court ruling.[22]

OFAC designates two Gaza entities: On March 22, the Office of Foreign Assets Control (OFAC) blacklisted the Islamic National Bank of Gaza (INB) because it was controlled by Hamas and "patronized" by some of Hamas' military wing members. OFAC also designated Al-Aqsa Television, a television station in Gaza which is financed and controlled by Hamas. According to OFAC, the INB opened in Gaza city in April 2009 without a legal licence from the Palestinian Monetary Authority (PMA). Furthermore, the Palestinian Authority, the Palestinian Capital Market Authority and the PMA had publicly declared the bank illegal, claiming it was non-compliant with banking and securities regulations and warned the public against conducting any business with INB. OFAC also stated that the INB is providing Hamas with "means to receive and store large amounts of smuggled cash" for use at the group's discretion. In May 2009, after Hamas's finance office moved €1.1 million to INB, the group used the money to pay the salaries of members of its military wing. OFAC has also declared Al-Aqsa Television as Hamas's primary media outlet, airing programs designed to recruit children to become armed Hamas fighters when they reach adulthood. After Hamas was elected in January 2006, it contributed US$ 500,000 to the TV channel. As of late 2009, Hamas headquarters in Damascus, Syria, allocated hundreds of thousands of dollars to Al-Aqsa TV.[23]

Iran inaugurates Financial Intelligence Unit: On February 7, Iran inaugurated its newly established Financial Intelligence Unit (FIU) with the support of the United Nations Office on Drugs and Crime. The FIU, which follows international standards, will receive and analyze suspicious transactions submitted by financial institutions and banks in order to fight money laundering and terrorist financing. It is also expected to collaborate with FIUs from other countries. Funding from Germany, Italy and the United Kingdom helped finance various technical cooperation projects, which allowed Iran to improve its anti-money laundering and counter-terrorist financing framework.[24]

BIBLIOGRAPHY

1. "Ex-Fastweb chief sought in money laundering probe Scaglia and PdL Senator 'linked to huge scam'." *ItaliaInformazioni.com.* February 23, 2010.

"Laundering the Proceeds of VAT Carousel Fraud." *FATF – GAFI*, Financial Action Task Force. February 23, 2007.

"Probe into Italy mafia laundering." *Sydney Morning Herald*. March 8, 2010.

"Senator snapped with 'Ndrangheta boss Fastweb founder Scaglia coming back to 'clear things up'."

"Telecom Italia also cited in Laundering Probe." *lifeinitaly.com.* February 23, 2010. "Yevgeny Gurevich brought 2 billion euro through a "carousel"." *Russian Mafia.* February 12, 2010.

Boland, Vincent. "Fresh scandal embarrasses Telecom Italia." *Financial Times.* February 25, 2010.

Dinmore, Guy. "Complexity of 'fraud' boggles mind." *Financial Times.* March 6, 2010.

Povoledo, Elisabetta, and David Jolly. "Telecom Italia Delays Results Because of Money-Laundering Scandal." *IDG News Service.* February 26, 2010.

Willan, Philip."Italian telcos caught up in massive Mafia fraud." *IDG News Service.* February 24, 2010.

2. Swift, Aisling. "Feds investigate Naples man in money laundering probe tied to online gambling." *Naplesnews.com.* February 28, 2010.

Wolf, Brett. "German man admits he funnelled money to US on behalf of internet gambling firms." *Complinet.com.* February 28, 2010.

3. Alpert, Bill. "Small New Zealand Firm's Link to Smuggling Case." *Barron's Online.* January 4, 2010.

Alpert, Bill. "Blowing the Whistle--and Paying the Price." *Barron's Online.* March 9, 2010.

Alpert, Bill. "Aiding the Drug Cartels." *Barron's Online.* March 22, 2010.

Anderson, Curt. "Wachovia paying $160M to settle case involving laundering of Mexican drug money." *The Associated Press.* March 17, 2010.

Global Press Service. "New Zealand: Drug money launderer linked to NZ company." *Complinet.* February 12, 2010.

Global Press Service. "New Zealand: Fears 'firms' are laundering terrorist cash." *Complinet.* January 8, 2010.

Monroe, Brian. "Wachovia Will Pay Record $160 Million to Settle Casas de Cambio Case." *moneylaundering.com.* March 17, 2010.

4. Direct News. “FIFA aims to tackle money laundering with new transfer system”. *Complinet.* February 24, 2010.

5. Monroe, Brian. “Free Trade Zones Vulnerable to Laundering, Tax Evasion: FATF”. *Moneylaundering.com.* March 31, 2010.

6. Fischer, Howard. "State to get Millions in suit over money sent to Mexico." *Capitol Media Services.* February 12, 2010.

Monroe, Brian. "Western Union Pays $94 Million to Settle Lawsuit Tied to Laundering, Human Trafficking."

7. Adams, Colby. “Fueled by Recession, Use of “Factoring” to Launder Money Grows in Latin America”.

DLA Piper. “JMLSG publishes guidance on invoice finance”. *Money Laundering Law.* November 2007.

8. Adams, Colby. "IMF Launches Program to Stem Laundering Through Precious Metals." *moneylaundering.com.* March 23, 2010.

9. Monroe, Brian. "FinCEN Expands 314(a) Bank Information Sharing Program to Foreign Law Enforcement." *moneylaundering.com.* February 5, 2010.

10. "Regulatory Gap Leaves Some MSBs, Casinos With Little Sanctions Oversight." *moneylaundering.com.* January 14, 2010.

11. Wolf, Brett. “New ‘Trade Transparency Unit’ in Panama to join fight against trade-based money laundering”. *Complinet.* March 4, 2010.

12. "PayPal halts some India payments." *BBC News.* February 11, 2010.

Irani, Farhad. "New Bank Withdrawal Instructions for Our Customers in India." *The PayPal Blog.* March 1, 2010.

Qing, Liau Yun. "PayPal India to resume fund withdrawals." *Digital Media.* March 1, 2010.

Ribeiro, John. "PayPal Suspends Personal Payments to India." *IDG News Service.* February 8, 2010.

13. Brockner, Eliot. "Ecuador Blacklisted for Money Laundering." *ISN Security Watch.* April 6, 2010.

Dorsey, James M. "Ecuador emerges as hub for international crime." *Deutsche Welle.* February 2, 2010.

14. Coyle, Martin. "Report warns of dangers of Russian 'grey practices'." *Complinet.* March 26, 2010.

Owen, James, and Rosie Hawes. "Grey practices in the Russian business environment." Control Risks. March 11, 2010.

15. Freeze, Colin. "Extremists: Canada adds al-Shabab to its terrorist list Crown can now seize money and assets of front operation here." *Globe and Mail.* March 8, 2010.

16. “Prison à vie pour le terroriste de Maskinongé”. *Le Journal de Montréal.* February 18, 2010.

"Quebecer in bomb plot gets life sentence." *CBC News.* February 17, 2010.

Block, Irwin. “Quebec man gets life for terror activity”.
The Ottawa Citizen. February 18, 2010.

Desjardins, Christiane. “La perpétuité demandée pour Saïd Mamouh”. *Le Soleil.* November 14, 2009.

17. "Treasury Targets Iran's Islamic Revolutionary Guard Corps."
U.S. Department of Treasury. February 10, 2010.

18. Kelly, Cathal. "More SUVs among top 10 stolen vehicles."
The Toronto Star. December 9, 2010.

Hanon, Andrew. “Auto Theft Terror”. *Edmonton Sun*. January 21, 2010.

19. Monroe, Brian. "New York Prosecutors Indict Three for Allegedly Running Iranian Hawala."
moneylaundering.com. January 20, 2010.

Wolf, Brett. "Feds take down Manhattan 'hawaladar' who allegedly transferred millions of dollars to Iran."
Complinet. January 12, 2010.

20. "3 men charged in Miami with illegally exporting products to South America to finance Hezbollah."
The Canadian Press. February 19, 2010.

"Seven Charged with Illegal Export of Electronics to U.S.-Designated Terrorist Entity in Paraguay."
Federal Bureau of Investigation Miami. February 19, 2010.

Wolf, Brett. "Miami men did business with 'global terrorist' in Paraguay, prosecutors say."
Complinet. February 24, 2010.

21. Valiquette, Joe. "Manhattan's U.S. Attorney Creates Counter-Terror, Drug Unit."
DNAinfo. January 18, 2010.

22. Monroe, Brian. "U.K. Lawmakers to Quickly Bolster Sanctions Law After Supreme Court Ruling."
Moneylaundering.com. January 27, 2010.

23. Wolf, Brett. "OFAC targets Gaza entities with alleged ties to Hamas."
Complinet. March 22, 2010.

24. “Iran’s Financial Intelligence Unit inaugurated with UN assistance”.
Complinet. February 8, 2010.