

July 7, 2006

Compilation of publicly available statements regarding the monitoring of wire transfers by the U.S. government

I. It was public knowledge that wire transfers including SWIFT, CHIPS and Fedwire transactions were being monitored by the United States Government

A. Multiple newspaper articles and testimonies revealed the existence of government searches for terrorist activity in SWIFT and similar wire transfer databases long before the New York Times article

“Funding on that scale would not necessarily have required large international bank transfers of the kind often seen in cases involving drug cartels or corrupt regimes. That could limit the ability of the National Security Agency to follow the money through its electronic intercepts of such transactions, which are carried out by the Society for Worldwide Interbank Financial Telecommunications (SWIFT), headquartered in Belgium.”

The Baltimore Sun, September 21, 2001

“Jimmy Gurule, the US Treasury's undersecretary of enforcement, said the FATF would consider urging member countries to adopt a range of measures to end terrorist financing within their borders by better tracking cross-border payments and remittances.

The measures include:

* Proposals requiring financial institutions to file suspicious activity reports on funds they believe are being held for terrorist groups.

* Registering informal money exchange agents and requiring them to record the names and addresses of those making payments.

* Reporting detailed information on international wire transfers.”

Financial Times, London Edition, October 23, 2001

“Finally, I can report that starting on September the 17th last year, the New York Reserve Bank, at the request of law enforcement and pursuant to subpoenas began searching the records of FedWire (ph) the Federal Reserve's large dollar electronic payment system for information related to the terrorist acts.

Search results have been provided to various law enforcement agencies, which have reported to

us that the information we provided, has been useful to their law enforcement and ongoing investigations.”

Richard Spillenkothen, Director, Banking Supervision and Regulation Division, Federal Reserve System
Senate Hearing of the Housing and Urban Affairs Committee, January 29, 2002

“I think we already have at the credit union level a lot of policies and security procedures that are in place to track suspicious movements -- for -- I'll give you an example. Wire transfers, which is one of the most popular services we provide in my credit union. Every time we do a wire transfer overseas we match that name against the list of OFAC.”

John Herrera, Vice President, Lation-Hispanic Affairs, Self Help Credit Union,
Representative, Credit Union National Association and World Council of Credit Unions
Hearing of the Oversight and Investigation Subcommittee of the House Financial Services Committee,
February 12, 2002

“To date, over 1000 search warrants have been executed and numerous subpoenas have been served seeking information on over 10,500 persons or accounts. Over 321,000 documents have been processed and over 2,450 accounts have been examined, including more than 90 foreign bank accounts. In addition, analysts have reviewed over 940 credit card accounts and scrutinized more than 13,000 domestic and foreign wire transfers. While the analysis continues, through financial information, we have established how the hijackers received their money, how and where they were trained to fly, where they lived and - perhaps most significantly - the names and whereabouts of persons with whom they worked and came into contact.”

Mary Lee Warren, Deputy Assistant Attorney General, February 12, 2002

“Dennis Lormel, head of the FBI's financial crimes section, said agents have reviewed and documented more than 66,000 financial transactions and 4,300 foreign wire transfers conducted by suspected terrorists in the U.S. and around the world.”

The Toronto Sun, February 22, 2002

“OFAC has widely disseminated the names of new designated terrorists to the business and financial communities through websites, Fedwire Alerts, CHIPS system notices, communications to Federal and State regulators, and electronic broadcasts to 175 key industry groups. Information on terrorist designations is also distributed to the public by way of Customs, the Government Printing Office, and other agency networks.”

-Jimmy Gurule, Under Secretary for Enforcement of U.S. Department of the Treasury,
House Hearing of the Appropriations Committee, February 27, 2002

“Messages are scanned field by field and OFAC-Agent determines if there is any such element (referenced by its name/address, or its SWIFT code, or any keyword) which generates a "hit" against watch lists. OFAC-Agent has been designed to be able to use any number of lists (international, national, tailored in the bank) and takes into account new versions of the lists without extra tuning.

STB-Detector is the first to anti-money laundering application to combine several key controls in one package, specifically: applying very detailed account opening controls, secondly tracking and

profiling of all account activity - not just wire transfers, and thirdly managing review and follow-up workflows of suspicious or poorly documented transactions.”
M2 Presswire, July 9, 2002

“Bottomline Technologies has released WebSeries OFAC (Office of Foreign Asset Control), a new application module of its Web-based Universal Payment Engine that can spare organizations up to \$ 1 million in fines and jail time by helping them comply with the Patriot Act, new legislation that bars organizations from conducting transactions with known terrorists.

WebSeries OFAC automatically tracks all types of transactions at the enterprise level -- including Fedwire, SWIFT, ACH (automated clearing house) and check payments -- against the OFAC list. Most banks only match their Fedwire and SWIFT payments.”

-The Financial Executive, September 1, 2002

“Statistics compiled by the government establish an unprecedented level of investigative activity relating to the tracing of terrorist assets and related money laundering activity. In light of the breadth of these governmental inquiries, it is clear that law-abiding companies are being called upon to supply records and information about customers, clients, and transactions like never before. Since September 11, over 1,000 search warrants have been served, and records relating to over 10,500 persons and accounts have been subpoenaed. More than 2,450 accounts have been reviewed, including more than 90 accounts that related to foreign banks. More than 13,000 domestic and foreign wire transfers have been reviewed.”

EIU ViewsWire, September 27, 2002

“As touched upon earlier, a significant focus of the TFOS' efforts is prediction and prevention. In this regard, it has developed numerous data mining projects to provide further predictive abilities and maximize the use of both public and private database information. These efforts are complemented by the centralized terrorist financial database which the TFOS developed in connection with its coordination of financial investigation of individuals and groups who are suspects of FBI terrorism investigations. The TFOS has cataloged and reviewed financial documents obtained as a result of numerous financial subpoenas pertaining to individuals and accounts. These documents have been verified as being of investigatory interest and have been entered into the terrorist financial database for linkage analysis. The TFOS has obtained financial information from FBI Field Divisions and Legal Attache Offices, and has reviewed and documented financial transactions. These records include foreign bank accounts and foreign wire transfers. The information contained within the aforementioned database is being used to identify terrorist cells operating in the United States and abroad to prevent further terrorist acts. The TFOS meets regularly with representatives from the banking community and the financial services industry to share information and to refine methods to detect and identify potential terrorists around the world.”

Dennis Lormel, Financial Crimes Section Federal Bureau of Investigation,
Senate Hearing of the Judiciary Committee, October 9, 2002

“Banks are in a quandary over the USA PATRIOT Act's tough deadlines for compliance with information requests from law enforcement agencies under the Bank Secrecy Act. The USA

PATRIOT Act places a 120-hour time limit on a bank's response to such requests.

The deadline is especially troublesome for smaller banks which, typically lacking an automated solution, must instead plow through paper records for occurrences of a suspect's name.

"To record [a wire transfer] is one thing, but to retrieve it is another," said Dave Kvederis, president and CEO of Bankserv, a San Francisco-based software firm. "You can record it on hunks of paper and put it in file cabinets, but if you need to find history on two years [of transactions] that can be more problematic."

Bank Systems & Technology, November 1, 2002

"We complement such direct law enforcement action with law enforcement support. Through FinCEN, Treasury serves as a repository and analytical hub for Bank Secrecy Act information, which aids investigators across the interagency community in finding financial links to criminal enterprises and terrorist networks. Since February 2003, we have also used Section 314(a) of the Patriot Act to enable law enforcement, through FinCEN "Blastfaxes" to more than 31,800 financial institutions as of April 27, 2004, to locate quickly the accounts and transactions of those suspected of money laundering or the financing of terrorism. Since Section 314(a)'s creation, the system has been used to send the names of 1,712 persons suspected of terrorism financing or money laundering to financial institutions, and has resulted in 12,280 matches that were passed on to law enforcement. We understand the sensitivity of the use of this system, and will continue to ensure through vigorous review that this system is used only in cases where terrorist financing is suspected, or in the most egregious money laundering cases."

Dennis Glaser, Director of Executive Office for Financing and Financial Crime,
Hearing of the House Government Reform Subcommittee on Criminal Justice, Drug Policy, and Human Resources, May 11, 2004

"Obeying a mandate from the intelligence reform bill passed by Congress in December, the U.S. Treasury has begun pushing for access to millions of foreign banking and banking transfer records in an effort to track down terrorist financing. The agency has identified wire transfers in particular as the medium of most of these transactions and wants direct insight into the vast volumes of data flowing daily through services like SWIFT and Western Union."

Securities Industry News, May 9, 2005

"An agreement announced today between Information Technology, Inc. (ITI), a subsidiary of Fiserv, Inc. (Nasdaq:FISV), and GlobalVision Systems, Inc., will provide bankers with an advanced solution to help them comply with federal requirements outlined in the USA PATRIOT Act and Bank Secrecy Act (BSA).

In addition to automating the detection, investigation, monitoring and filing of Suspicious Activity Reports, Premier Patriot Officer also helps identify high-risk customers through multidimensional risk scoring. "All wire transfers are confirmed and SWIFT transactions are evaluated against the list published by the U.S. government," said Deterding."

Business Wire, May 23, 2005

“Australia is planning to address FATF's findings through two pieces of legislation, the Criminal Code Act of 1995 and the Transaction Reports Act. The proposed reforms will make it unnecessary for precursor events, such as an investigation by the Australian Crime Commission, for filing a Suspicious Transaction Report--the equivalent of an SAR in the U.S.--to trigger an investigation. More customer detail will also be required in international funds transfers, or wire transfers, submitted into and out of Australia, applying to all remittance services. A spokesperson for the Australian Transaction Reports & Analysis Center, the country's AML regulator, said, "While these cash dealers should not materially affect those cash dealers using Swift payments, it may impact non-Swift remitters."”

Securities Industry News, March 15, 2006

B. Other nations were open about their monitoring of wire transfers

“The Financial Transactions Reports Analysis Centre (FinTrac), the Canadian government agency that combats money laundering and terrorist finance says that it has gotten well beyond the simple matching of names in analyzing wire transfer data to identify patterns suggestive of criminal activity.

"We're not simply running watch lists against that data," says Peter Lamey, a FinTrac spokesperson in Ottawa. "The Swift messages can be parsed, they do contain fields, they can be formatted in a way that makes them useful for analysis. We're combining that data with other forms of transaction reports but also with other intelligence we get from law enforcement's financial intelligence units." Lamey says FinTrac also tries to identify anomalies within the transactions, and expects that it will get better at it as it collects more data for analysis.

Take the data fields in the MT-100 message format, which, according to Lamey, is primarily used for wire transfers. "It's not all open text," he says. "There are actually numeric tags with two digits so you can identify the sender, the bank identifier codes--and we're able to handle that through the fields in the Swift messages. Each of the different tags highlights a four-, two- or one-line field, and the fields have a set length of 35-40 characters. But they are alphanumeric."

The yield of such analysis can be triangulated with other intelligence, Lamey says. "We're running that data and combining it with other information that we have--other forms of transaction reports but also other intelligence we get from law enforcement or other financial intelligence units."

Lamey concedes that the loose handling of wire transfers does not help matters. "Even in wires with unintelligible alphanumeric data, there's enough information in there to get the money overseas," he notes. "You have to know the beneficiary, and although it's left blank sometimes, you have to know the sender. You have two parties to a transaction, you have a value and you have accounts. If there's other activity going on in the account at the other side, or if it links up to an account that has some other investigation or analysis, the matches can be made that way."

Such data might not actually be collected in the U.S. for several years. Meanwhile, "the Australians are further along than we Canadians," Lamey says. A spokesperson for AusTrac, the Australian money-laundering agency, could not be reached for comment.

Canada made it obligatory to report the movement of currency across its border two years ago. Says Lamey: "The reporting of wire transfers is all about money crossing the border, the use of MT-100 Swift messages is all about money crossing the border. Whether it crosses in a suitcase or a wire transfer, there's an obligation to report it."

Securities Industry News, May 9, 2005

"Organisations meeting in Singapore to coordinate the fight against money laundering and the financing of terrorism yesterday went public with their strategy.

Their first aim is to ensure total openness about exactly who is sending and receiving money...

Mr McDonnell said previous international wire transfers through the Swift system did not require the sender or recipient to be identified.

He said many APG countries have agreed to comply with the revised recommendation on providing the identities of the sender and recipient but would need 12 months to implement the measure because it requires new laws."

The Business Times Singapore, June 11, 2005

"There is a strong commitment by FATF and the international community (to) ensure that these new international standards are adhered to," he said. The US passed tough legislation last week to curb terrorist financing and has stepped up pressure on other countries to follow that lead. That would include making the financing of terrorist activity a criminal offence, co-operating in law-enforcement efforts and strengthening customer identification for wire transfers."

Financial Times, London Edition, November 1, 2001

II. The Bush Administration has repeatedly acknowledged that it has relied on international cooperation and cooperation with the financial sector to monitor international wire transfers.

On October 22, 2001, Jimmy Gurule, Undersecretary of the Treasury for Enforcement, in a speech at the Crystal Gateway Marriott, put forward the proposals to be discussed by the Financial Action Task Force plenary meeting: "7. International Wire Transfers— Countries should take measures to require financial institutions and money remitters to include originator information...on funds transfers and related messages..."

On October 31, 2001, Mr. Gurule stated: "FATF [the Financial Action Task Force] adopted eight special recommendations which specifically target the ability of terrorists to generate income for their organizations, thus isolating the terrorists financially...[The recommendations] chart new territory by requiring countries to crack down on alternative remittal

systems such as hawalas, customer identification measures for wire transfers, and insuring that charities are not misused to finance terrorism.”

On November 7, 2001, Treasury Secretary Paul O’Neill stated in a White House briefing, “[The terrorists] know that we are watching, and for that reason, they try to funnel their money through undocumented, unregulated financial networks constructed to bypass the civilized world’s detection. But their system is imperfect. Somewhere, it must always interface with modern banking and finance. When that connection is made, we have the wherewithal to intervene, and thanks to the cooperation of allies and coalition partners...we have begun to act.”

On December 31, 2001, Mr. Gurule, in an article in *Hispanic* entitled “An Unconventional Strategy for an Unconventional War,” wrote, e “FTAT [the Foreign Terrorist Asset Tracking Center] is dedicated to identifying the financial infrastructure of terrorist organizations worldwide and curtailing their ability to move money through the international banking system.”

On February 12, 2002, Juan C. Zarate, Deputy Assistant Secretary, Terrorism and Violent Crime, U.S. Department of Treasury, testified to the House Financial Services Committee: “Terrorist groups, including al-Qaeda, use different means of moving money to support their respective organizations. This money movement around the world, which largely still relies on traditional wire transfers, provides the footprints to where sleeper cells lie and allows us to attempt to disrupt those fund flows... The Treasury Department continues to monitor the use of shell bank, shell companies, and correspondent accounts to move illicit funds directed for terrorist financing purposes... Some U.S. banks have voluntarily closed correspondent accounts with foreign-based banks when there have been suspicious wire transfers...”

On July 31, 2003, FBI Acting Assistant Director for Counterterrorism John Pistole testified before the Senate Governmental Affairs Committee, “What TFOS [the Terrorist Financing Operation Section] has been doing is trying to follow the money, to identify those individuals who may be involved in terrorist financing and then to trace that money with law enforcement intelligence aspects...One of the key areas has been our outreach with, and cooperation from, the private sector. In that area, for example, we have developed the ability to conduct real-time monitoring, and specifically identified financial activity, which has been invaluable not only to investigations here in the US, but to some of our foreign partners, who have relied on that information, tracking money going from the US overseas that may be used in terrorist activity, or vice versa.... At the request of a foreign liaison service, TFOS traced financial transactions in a near realtime manner which led to the location of a terrorist cell and prevention of a terrorist attack.”

On September 29, 2004, John E. Lewis, Deputy Assistant Director, FBI Counterterrorism Division, testified to the Senate Banking, Housing, and Urban Affairs Committee, “Efforts to counter the use of the informal banking system include...requiring money transmitting businesses, which include any person who engages as a business in the transmission of money, to register with the Financial Crimes Enforcement Network (FinCEN).

The Bush Administration has also corroborated that, as Ron Suskind reports in *The One Percent Doctrine*, terrorists have become aware that wire transfers are being monitored and are changing how they move money internationally.

On April 4, 2006, Assistant Secretary of State for Economic and Business Affairs E. Anthony Wayne testified to the Senate Banking, Housing, and Urban Affairs Committee: “One anecdotal measure of the success of our present coalition buildings is the increasing use by terrorist financiers of riskier, more difficult and expensive means in preference to the more horrible international financial system. Abuses of charities, of not-for profit organizations, of cash couriers, of wire transfers and other alternative remittance systems have become an increasing focus of our discussions and our cooperation with our international partners”

III. Congress has given the President the authority to monitor the international electronic transfer of funds to gain intelligence on terrorists, and Treasury has been openly working on regulations to do so.

Immediately following the Sept. 11 Attacks in 2001, Congress publicly declared its intention to provide the US government with legislative tools to monitor the international flow of terrorist money.

In House Financial Services Committee Hearing on October 3, 2001, Chairman Michael Oxley stated, “Members of this committee will introduce comprehensive anti-terrorism and money laundering legislation that focuses on three major goals:

- bolster law enforcement’s ability to find and destroy the financing of terrorist organizations, whether in banks or underground ‘hawala’ systems;
- establish a government-industry partnership to stop terrorist funding in real-time; and
- track any terrorist money kept in secret offshore havens and increase foreign cooperation with U.S. efforts.”

Congress openly deliberated in 2004 whether authorizing the Treasury department to monitor international wire transfers would be useful.

From a Hearing of the House Financial Services Committee on August 23, 2004:

REP SUE KELLY (NY): “The committee is familiar with the ability of CENTRAC, the Canadian financial intelligence unit, and AUSTRAC, the Australian FIU, to receive international wire-transfer data electronically. Wouldn’t this be helpful for our FIU in Treasury, the FinCEN, to be able to have that authority?...”

STUART LEVEY, TREASURY UNDERSECRETARY FOR TERRORISM AND FINANCIAL INTELLIGENCE:” I do think this is something that I know [FinCEN Director] Bill Fox is looking at very carefully. It does, frankly, appear to me to be something that would be useful. I’m a little hesitant to jump in without knowing the details. It does seem to me there may be a scalability problem...given the volume that we have to deal with...”

REP KELLY (NY): “If you need more money to get the job done electronically, I think we must address that her in Congress, and we need to do it rapidly.”

From a Hearing of the House Financial Services Committee on September 22, 2004:

REP SUE KELLY (NY): “We’re here because of our shared commitment to strengthening our ability to track and take out the financial support systems of the terrorists...In the coming days, this committee should also focus on our ability to collect and analyze information regarding cross-border fund transfers. As members of this committee recall, the 9/11 commission clearly articulated the direct relevance of international wire transfers to terror finance. We need to do more to ensure that our wire transfer systems are not being used for illicit purposes.”

* * *

REP SUE KELLY (NY): “As you know, the United States lags behind other countries in our ability to deter and detect the misuse of these international funds transfer systems for illicit purposes...In fact, some U.S. authorities have suggested that a well-structured reporting requirement for international wire transfers would do more to address terrorist financing than any other change to the Bank Secrecy Act. Since money laundering and terror finance are inherently international, and law enforcement’s ability to trace funds is curtailed to find from where the funds originate or transit to other countries, my question is, what impact would having this authority have on our government’s ability to fight terrorist financing?...”

STUART LEVEY, TREASURY UNDERSECRETARY FOR TERRORISM AND FINANCIAL INTELLIGENCE: “I’d like to say two things in response to that. One is that it may well be that that authority is one that would be beneficial to us with respect to combating terrorist financing, money laundering, and particularly helping us with ongoing investigations...The authority may well be useful. And the reason I can’t be stronger is I just need to make sure that what we do is something that we’re capable of taking in. In other words, I don’t want to require the reporting of a lot of information that we don’t have the capacity to use and analyze at this point...”

REP KELLY: “Mr. Levey, we stand ready and willing to work with you to see if there isn’t something more we can do to identify these cross- border transmittals and get them into some kind of position where they are going to work as flags to help us regarding terror.”

At the end of 2004, Congress passed the Intelligence Reform and Terrorism Prevention Act (S.2845, P.L. 108-458), which authorized the Treasury Department to develop regulations requiring financial institutions to give the government information on cross-border electronic money transfers. This legislation provided the framework within which the administration was supposed to conduct its monitoring of this financial information.

Title VI, Subtitle D, Sec. 6302:

Paragraph 1: “IN GENERAL: The Secretary shall prescribe regulations requiring such financial

institutions as the Secretary determines to be appropriate to report to the Financial Crimes Enforcement Network certain cross-border electronic transmittals of funds, if the Secretary determines that reporting of such transmittals is reasonably necessary to conduct the efforts of the Secretary against money laundering and terrorist financing.”

Paragraph 4: “FEASABILITY REPORT . A. Before prescribing the regulations required under paragraph (1), and as soon as is practicable after the date of enactment of the National Intelligence Reform Act of 2004, the Secretary shall submit a report to the Committee on Banking, Housing, and Urban Affairs of the Senate and the Committee on Financial Services of the House of Representatives that –

i) identifies the information in cross-border electronic transmittals of funds that may be found ...to be reasonably necessary to conduct the efforts of the Secretary to identify money laundering and terrorist financing...

ii) outlines the appropriate form, manner, content, and frequency of filing of the reports that may be required under such regulations;

iii) identifies the technology necessary for the Financial Crimes Enforcement Network to receive, keep, exploit, protect the security of, and disseminate information from reports of cross-border electronic transmittals fo funds to law enforcement and other entities...

iv)discusses the information security protections required by the exercise of the Secretary’s authority under this section.

Following the enactment of this law, the Treasury Department publicly sought to engage in the monitoring of international wire transfers, along with the feasibility study mandated by Congress.

On April 6, 2006, Stuart Levey, Treasury Under Secretary for Terrorism and Financial Intelligence, testified to Congress about the need for “Development funding for FinCEN’s Cross-Border Wire Transfer System Initiative. The authorizing language (Section 6302 of the Intelligence Reform Act of 2004 (S.2845 P.L. 108-458)) presents the Bureau with two tasks (1) a feasibility study to be completed as soon as practicable; and (2) the implementation of enabling regulations and a technological system for receiving, storing, analyzing, and disseminating the reports...”

This testimony clearly establishes the existence of Treasury plans to monitor cross-border wire transfers. Meanwhile, it was widely reported in the press that the Treasury Department was discussing the feasibility of the new monitoring of wire transfers with financial institutions and regulators.

On April 11, 2005, Eric Lichtblau of the New York Times reported, “The Bush administration is developing a plan to give the government access to possibly hundreds of millions of international banking records in an effort to trace and deter terrorist financing, even as many bankers say they already feel besieged by government antiterrorism rules...

“The initiative, as conceived by a working group within the Treasury Department, would vastly expand the government’s database of financial transactions by gaining access to logs of

international wire transfers in and out of U.S. banks....

“Government officials said that *the effort, which grew out of a brief, little-noticed provision in the intelligence reform bill [S.284 IRTP Act above] passed by Congress in December*, would give them the tools to track leads on specific suspects and, more broadly, to analyze patterns in terrorist financing and other financial crimes...

“The provision authorized the Treasury Department to pursue regulations requiring financial institutions to turn over ‘certain cross-border transmittals of funds’ that might be needed in combating money laundering and terrorist financing.

“The plan for tracking overseas wire transfers is likely to intensify pressure on banks and other financial institutions to comply with the expanding base of provisions to fight money laundering, industry and government officials agreed.”

On March 10, 2006, Jeannine Aversa of the AP Financial Wire wrote: “The Bush administration is exploring the idea of requiring financial institutions to provide information on electronic transfers of money in and out of the United States, saying it might help catch terrorist financiers and money launderers.

“The Treasury Department’s Financial Crimes Enforcement Network said Friday it is seeking input on the matter from the banking and financial services industry.

“‘If we can identify data in cross-border wire transfer records that helps protect economic and national security and find a workable way to efficiently collect the data...it will enormously strengthen our efforts,’ said Robert Werner, director of FinCen....

...the agency also is issuing a survey to industry groups to get feedback on these and other issues.”

Both financial institutions and their regulators in the government offered resistance to the Treasury Department’s proposals.

On April 11, 2005 the Eric Lichtblau of the New York Times reported: “The aggressive tactics...have already caused something of a backlash among banking compliance officers and even some federal officials, who say the effort has gone too far in penalizing the financial sector for lapses and has effectively criminalized what were once seen as technical violations.”

On **June 21**, 2006, Stacy Kaper of American Banker reported: “Requiring banks to report all international wire transfers to the government could hinder innovation in the U.S. payments system, significantly increase regulatory burden, and raise privacy concerns, regulators told the Financial Crimes Enforcement Network last week.

“Since last year FinCen has been studying whether to recommend that banks comply with such a requirement, and during the past two months it sought input from federal regulators...

“They also asked FinCen to conduct a more thorough review of law enforcement officials’ ability to use the data to crack down money laundering and terrorist financing.

“FinCen has said that such data also could be useful to regulators, but the agencies seemed skeptical. They noted that bank examiners already have access to cross-border wire transfer data during examinations, sources said...

“Industry representatives continue to oppose any such reporting requirement and hope the

regulators' concerns will resonate with Fincen. But many industry sources said FinCen appears to be marching forward regardless."

Thus, it was well known that Treasury intended larger-scale monitoring of wire transfers.

IV. Ron Suskind, in *The One Percent Doctrine*, published by Simon and Schuster on June 20 (two days before the Times allegedly revealed the information) explained at length that the Bush administration was tracking wire transfers, and Western Union in particular, since 2001 as part of the "financial war" on terror.

November 2001: "[Treasury Department General Counsel David] Aufhauser, and his fellows, were trying to cut off to cut off the flow of funds to terrorists, carrying forward the President's "financial war" pledge. [Section Chief of FBI Terrorist Financing Operations Section, Counterterrorism Division Dennis] Lormel was trying to use money as intelligence to find and stop terrorist operations."

–Ron Suskind, *The One Percent Doctrine*, p. 142

"The most effective coordination of resources, manpower, and ingenuity in the U.S. government had been in the financial realm... Western Union had been the most efficient part of that effort....Requests for Western Union assistance started to come to FBI from 'down the river' at CIA. Western Union was asked for historical data on clients in more and more areas of interest."

–Ron Suskind, *The One Percent Doctrine*, p. 208-9

"For [financial intelligence], the administration relied heavily on First Data. Covenants with other credit card processors in the United States and abroad meant that—much like large telecom switches—everything could be invisibly blended... Western Union had similar sharing arrangements for wire transfers...to clear or trace transactions, large companies generally have access to one another's back office processing units....You just need a universal passport—like the one Western Union possesses...In the first few weeks after the [9/11] attacks, thousands of financial searches were conducted based on initial communications leads from NSA."

–Ron Suskind, *The One Percent Doctrine*, p. 38

It was further reported that the goal of tracking the wire transfers is not necessarily to freeze terrorist assets, but to gather information on the location and infrastructure of terrorist organizations.

"Initiatives launched by Treasury and CIA were getting much better at tracking money as it passed through accounts across the world... Money, they now all understood was for the most part a form of intelligence...The money trail..could identify the players, the place, and, possibly, the intent."

–Ron Suskind, *The One Percent Doctrine*, p. 143

“Day by day, U.S. officials grew to appreciate that they *wanted* cash to flow—manageably, modestly flow—so they’d have something to follow. On an intelligence-scarce landscape, *money was intelligence.*”

—Ron Suskind, *The One Percent Doctrine*, p. 208

In some cases, Suskind reported very specifically on operational details of the use of Western Union information.

“Lormel and his partners at FBI pushed deeper. What about real-time information—transactions as they occur? And photos? Western Union had pinpoint cameras in some of its offices. Just as someone making an ATM transaction is photographed, so, often, is the sender of a wire transfer, and the recipient, though they often don’t know it.”

—Ron Suskind, *The One Percent Doctrine*, p. 209

Suskind then describes, on pages 230-33, a specific use of this power against Palestinian Islamic Jihad terrorists:

“[Israel Intelligence Service Shin Bet Director Avi] Dichter gave the United States a piece of intelligence to begin the process: the name of a supporter of Palestinian Islamic Jihad who was expected to wire money from Lebanon to a point somewhere in Israel. Early in April, Western Union’s Offices in Lebanon received the expected order....In an arrangement with the U.S. Federal Court for the Eastern District of Virginia...[the Terrorism Section of the Department of Justice] issued an instantaneous subpoena. It allowed Western Union...to notify FBI and CIA about which location the money was being wired to, and who was picking it up. All of it occurred in minutes. Israeli intelligence officers were hailed. They raced, silently, to the right Western Union office in Hebron, and then followed the PIJ courier to his safe house in the West Bank. From there, electronic surveillance equipment swiftly tracked communications to other cells in the Palestinian territories.

“Two further wire transfers were targeted in early May. And, each time, the golden disclosure has handed by the U.S. government to Israeli forces...”

Terrorists have learned about this in 2003, and have since started moving their money in other ways.

“In the closing months of 2003, we started to go blind. The U.S. government, that is. The carefully constructed global network of sigint [signals intelligence] and what can be called finint, or financial intelligence, started to go quiet. In short, al Qaeda...stopped leaving electronic footprints...They were going underground.”

—Ron Suskind, *The One Percent Doctrine*, p. 277

“Eventually, and not surprisingly, our opponents figured it out... ‘We were surprised it took them so long,’ said one senior intelligence official... The al Qaeda playbook, employed by what was left of the network, its affiliates and imitators, started to stress the necessity of using couriers to carry cash and hand-delivered letters.”

—Ron Suskind, *The One Percent Doctrine*, p. 278

“The FBI ran a few more wire transfer traps through Western Union for [Israel Intelligence Service Shin Bet Director] Avi Dichter– one in August, another in October–but it seemed like the prey among the Palestinian leadership was finally getting wise.”

–Ron Suskind, *The One Percent Doctrine*, p. 281

Monitoring wire transfers was made illegal by FISA in 1978.

“During World War II, all U.S. telegraph companies forwarded copies of international cables to the federal government. The program, “Operation Shamrock,” continued after the war and was unknown to Congress and top intelligence officials...This collection of foreign intelligence also involved U.S. citizens and was blocked when it was uncovered, along with other intelligence abuses, during post-Watergate congressional investigations of CIA in the mid-seventies. Shamrock, and similar abuses in the wiretapping of U.S. citizens...was the impetus for the passage of the Federal Intelligence Surveillance Act in 1978, and the creation of the so-called “FISA Court.”

–Ron Suskind, *The One Percent Doctrine*, p. 35-6