

Published on Friday, June 23, 2006 by the [Los Angeles Times](#)

Secret U.S. Program Tracks Global Bank Transfers

The Treasury Dept. program, begun after the Sept. 11 attacks, attempts to monitor terrorist financing but raises privacy concerns.
by Josh Meyer and Greg Miller

The U.S. government, without the knowledge of many banks and their customers, has engaged for years in a secret effort to track terrorist financing by accessing a vast database of confidential information on transfers of money between banks worldwide.

The program, run by the Treasury Department, is considered a potent weapon in the war on terrorism because of its ability to clandestinely monitor financial transactions and map terrorist webs.

It is part of an arsenal of aggressive measures the government has adopted since the Sept. 11 terrorist attacks that yield new intelligence, but also circumvent traditional safeguards against abuse and raise concerns about intrusions on privacy.

Under this effort, Treasury routinely acquires information about bank transfers from the world's largest financial communication network, which is run by a consortium of financial institutions called the Society for Worldwide Interbank Financial Telecommunication, or SWIFT.

The SWIFT network carries up to 12.7 million messages a day containing instructions on many of the international transfers of money between banks. The messages typically include the names and account numbers of bank customers — from U.S. citizens to major corporations — who are sending or receiving funds.

Through the program, Treasury has built an enormous — and ever-growing — repository of financial records drawn from what is essentially the central nervous system of international banking.

In a major departure from traditional methods of obtaining financial records, the Treasury Department uses a little-known power — administrative subpoenas — to collect data from the SWIFT network, which has operations in the U.S., including a main computer hub in Manassas, Va. The subpoenas are secret and not reviewed by judges or grand juries, as are most criminal subpoenas.

"It's hard to overstate the value of this information," Treasury Secretary John W. Snow said Thursday in a statement he issued after The Times and other media outlets reported the existence of the Terrorist Finance Tracking Program.

SWIFT acknowledged Thursday in response to questions from The Times that it has provided data under subpoena since shortly after Sept. 11, 2001, a striking leap in cooperation from international bankers, who long resisted such law enforcement intrusions into the confidentiality of their communications.

But SWIFT said in a statement that it has worked with U.S. officials to restrict the use of the data to terrorism investigations.

The program is part of the Bush administration's dramatic expansion of intelligence-gathering capabilities, which includes warrantless eavesdropping on

the international phone calls of some U.S. residents. Critics complain that these efforts are not subject to independent governmental reviews designed to prevent abuse, and charge that they collide with privacy and consumer protection laws in the United States.

Steven Aftergood, director of the Project on Government Secrecy at the Federation of American Scientists, said the SWIFT program raises similar issues. "It boils down to a question of oversight, both internal and external. And in the current circumstances, it is hard to have confidence in the efficacy of their oversight," he said. "Their policy is, 'Trust us,' and that may not be good enough anymore."

A former senior Treasury official expressed concern that the SWIFT program allows access to vast quantities of sensitive data that could be abused without safeguards. The official, who said he did not have independent knowledge of the program, questioned what becomes of the data, some of it presumably related to innocent banking customers.

"How do you separate the wheat from the chaff?" the former official said. "And what do you do with the chaff?"

More than a dozen current and former U.S. officials discussed the program on condition of anonymity, citing its sensitive nature.

The effort runs counter to the expectations of privacy and security that are sacrosanct in the worldwide banking community. SWIFT promotes its services largely by touting the network's security, and most of its customers are unaware that the U.S. government has such extensive access to their private financial information.

U.S. officials, some of whom expressed surprise the program had not previously been revealed by critics, acknowledged it would be controversial in the financial community. "It is certainly not going to sit well in the world marketplace," said a former counterterrorism official. "It could very likely undermine the integrity of SWIFT."

Bush administration officials asked The Times not to publish information about the program, contending that disclosure could damage its effectiveness and that sufficient safeguards are in place to protect the public.

Dean Baquet, editor of The Times, said: "We weighed the government's arguments carefully, but in the end we determined that it was in the public interest to publish information about the extraordinary reach of this program. It is part of the continuing national debate over the aggressive measures employed by the government."

Under the program, Treasury issues a new subpoena once a month, and SWIFT turns over huge amounts of electronic financial data, according to Stuart Levey, the department's undersecretary for terrorism and financial intelligence. The administrative subpoenas are issued under authority granted in the 1977 International Emergency Economic Powers Act.

The SWIFT information is added to a massive database that officials have been constructing since shortly after Sept. 11. Levey noted that SWIFT did not have the ability to search its own records. "We can, because we built the capability to do that," he said.

Treasury shares the data with the CIA, the FBI and analysts from other agencies, who can run queries on specific individuals and accounts believed to have terrorist connections, Levey said Thursday in an interview with The Times.

Levey said that "tens of thousands" of searches of the database have been done over the last five years.

The program was initially a closely guarded secret, but it has recently become known to a wider circle of government officials, former officials, banking executives and outside experts.

Current and former U.S. officials said the effort has been only marginally

successful against Al Qaeda, which long ago began transferring money through other means, including the highly informal banking system common in Islamic countries.

The value of the program, Levey and others said, has been in tracking lower- and mid-level terrorist operatives and financiers who believe they have not been detected, and militant groups, such as Hezbollah, Hamas and Palestinian Islamic Jihad, that also operate political and social welfare organizations.

It's no secret that the Treasury Department tries to track terrorist financing, or that those efforts ramped up significantly after the Sept. 11 terrorist attacks. But the SWIFT program goes far beyond what has been publicly disclosed about that effort in terms of the amount of financial data that U.S. intelligence agencies can access.

The program also represents a major tactical shift. U.S. investigators long have been able to subpoena records on specific accounts or transactions when they could show cause — a painstaking process designed mainly for gathering evidence. But access to SWIFT enables them to follow suspicious financial trails around the globe, identifying new suspects without having to seek assistance from foreign banks.

SWIFT is a consortium founded in 1973 to replace telex messages. It has almost 7,900 participating institutions in more than 200 countries — including Bank of America, JP Morgan Chase Bank, Citibank and Credit Suisse. The network handled 2.5 billion financial messages in 2005, including many originating in countries such as Saudi Arabia, Pakistan and the United Arab Emirates that the United States scrutinizes closely for terrorist activity.

The system does not execute the actual transfer of funds between banks; that is carried out by the Federal Reserve and its international counterparts. Rather, banks use the network to transmit instructions about such transfers. For that reason, SWIFT's data is extremely valuable to intelligence services seeking to uncover terrorist webs.

CIA operatives trying to track Osama bin Laden's money in the late 1990s figured out clandestine ways to access the SWIFT network. But a former CIA official said Treasury officials blocked the effort because they did not want to anger the banking community.

Historically, "there was always a line of contention" inside the government, said Paul Pillar, former deputy director of the CIA's counterterrorism center. "The Treasury position was placing a high priority on the integrity of the banking system. There was considerable concern from that side about anything that could be seen as compromising the integrity of international banking."

Before Sept. 11, a former senior SWIFT executive said, providing access to its sensitive data would have been anathema to the Belgium-based consortium. But the attacks on the World Trade Center and the Pentagon led to a new mind-set in many industries, including telecommunications.

SWIFT said the Treasury Department's Office of Foreign Assets Control sent the first subpoena shortly after Sept. 11, seeking "limited sets of data" to learn about how Al Qaeda financed the attacks.

Unlike telephone lines and e-mail communications, the SWIFT network cannot be easily tapped. It uses secure log-ins and state-of-the-art encryption technology to prevent intercepted messages from being deciphered. "It is arguably the most secure network on the planet," said the former SWIFT executive who spoke on condition of anonymity. "This thing is locked down like Fort Knox."

SWIFT said it was responding to compulsory subpoenas and negotiated with U.S. officials to narrow them and to establish protections for the privacy of its customers. SWIFT also said it has never given U.S. authorities direct access to its network.

"Our fundamental principle has been to preserve the confidentiality of our users' data while complying with the lawful obligations in countries where we operate,"

SWIFT said in its statement.

Current and former U.S. officials familiar with the SWIFT program described it as one of the most valuable weapons in the financial war on terrorism, but declined to provide even anecdotal evidence of its successes.

A former high-ranking CIA officer said it has been a success, and another official said it has allowed U.S. counterterrorism officials to follow a tremendous number of leads. CIA officials pursue leads overseas, and the FBI and other agencies pursue leads in the United States, where the CIA is prohibited from operating.

Officials said the program is relied upon especially heavily when intelligence chatter from phone and e-mail intercepts suggested an imminent attack, conveying real-time intelligence for counterterrorism operations.

The former SWIFT executive said much can be learned from network messages, which require an actual name and address of both the sender and recipient, unlike phone calls and e-mails, in which terrorist operatives can easily disguise their identities.

"There is a good deal of detail in there," he said.

As the global war on terrorism has succeeded in taking out some senior terrorists and their financiers, particularly within Al Qaeda, the organization and its many affiliates have sought to move to hidden locations and to transfer their money through proxies such as charities, aid organizations and corporate fronts.

The officials said the SWIFT information can be used in "link analysis." That technique allows analysts to identify any person with whom a suspected terrorist had financial dealings — even those with no connection to terrorism. That information is then mapped and analyzed to detect patterns, shifts in strategy, specific "hotspot" accounts, and locations that have become new havens for terrorist activity.

The SWIFT program is just one of the Bush administration's post-Sept. 11 initiatives to collect intelligence that could include information on U.S. residents.

The National Security Agency, which can intercept communications around the world, is eavesdropping on the telephone calls and e-mails of some U.S. residents without obtaining warrants. And it has been accused of asking telecommunications companies to help create a database of the phone-call records of almost all Americans.

The Justice Department also has asked Internet companies to keep records of the websites customers visit and the people they e-mail for two years, rather than days or weeks, which would greatly expand the government's ability to track online activity.

Numerous lawsuits have been filed against the government and phone companies, challenging the NSA efforts. The government has asked courts to throw them out, invoking the "state secrets" privilege and arguing that trials would compromise national security. The NSA's interception of telephone calls also has been criticized for lacking an independent review process to ensure that the information is not abused.

The SWIFT program raises similar concerns, some critics say.

Privacy advocates have questioned "link analysis" because it can drag in innocent people who have routine financial dealings with terrorist suspects.

And no outside governmental oversight body, such as the Foreign Intelligence Surveillance Court or a grand jury, monitors the subpoenas served on SWIFT.

Levey said the program is subject to "robust" checks and balances designed to prevent misuse of the data. He noted that requests to access the data are reviewed by Treasury's assistant secretary for intelligence; that analysts can only access the data for terrorism-related searches; and that records are kept of each

search and are reviewed by an outside auditor for compliance.

Levey said there had been one instance of abuse in which an analyst had conducted a search that did not meet the terrorist-related criteria. The analyst was subsequently denied access to the database, he said.

During the last five years, SWIFT officials have raised concerns about the scope of the program, particularly at the outset, when it was handing over virtually its entire database. The amount of data handed over each month has been winnowed down.

"The safeguards were not all there in September 2001," Levey acknowledged. "We started narrowing it from the beginning."

New safeguards have been added, he said, noting that SWIFT officials are now allowed to be present when analysts search the data and to raise objections with top officials.

Officials from other government agencies have raised the issue of accessing the records for other investigative purposes, but Levey said such proposals have been rejected — largely out of concern that doing so might erode support for the program.

Asked what would prevent the data from being used for other purposes in the future, Levey said doing so would likely trigger objections from SWIFT and the outside auditor.

A SWIFT representative said that Booz Allen Hamilton, an international consulting firm, is the auditor but provided no further details on how the oversight process works.

Although the searches focus on suspected terrorist activity overseas, U.S. officials acknowledged that they do delve into the financial activities of Americans, noting that privacy laws don't protect individuals believed to be acting as a "foreign terrorist agent."

Officials said the administration has briefed congressional intelligence committees on the SWIFT program. In contrast, information on the NSA wiretapping was shared only with key lawmakers. One senior congressional aide said the committees have "a good handle on what the executive branch is doing to track terrorist financing" and are generally supportive of those efforts.

But the operation seems to have been kept secret from key segments of the banking industry, including senior executives in the United States and overseas.

John McKessy, chairman of the SWIFT user group in the United States, said he was unaware of any such program. McKessy represents companies and institutions that are not members of the SWIFT cooperative but use its messaging system.

SWIFT noted that its published policies clearly indicate that it cooperates with law enforcement authorities and that the subpoenas were "discussed carefully within the board," made up of members from 25 major banks. SWIFT said it has also kept informed an oversight committee drawn from the central banks of the major industrial countries.

The SWIFT program plugs a gap in global efforts to track terrorism financing.

In the United States, law enforcement authorities can access bank records if they get permission through the legal process. The FBI also has various legal ways to get almost instantaneous access to financial records. And U.S. banking laws require financial institutions to file Suspicious Activity Reports, but authorities believe Al Qaeda and other terrorist groups know how to evade the activities that trigger such red flags.

U.S. officials, however, long have complained that they cannot get access to financial records overseas and that some requests for cooperation from foreign governments and financial institutions took months, while others were rebuffed.

"The sort of 18th century notions on this stuff drive me nuts," said one senior U.S. counterterrorism official. "Somebody can move money with the click of a mouse, but it takes me six months to find it. If that is the world in which we live, you have to understand the costs involved with that."

The Sept. 11 commission urged the government in its July 2004 report on the U.S. intelligence failures leading up to the terrorist attacks to put more emphasis on tracking the flow of funds, rather than seeking to disrupt them, to learn how terrorist networks are organized.

Lee Hamilton, a former congressman and co-chairman of the commission who said he has been briefed on the SWIFT program, said U.S. intelligence agencies have made significant progress in recent years, but are still falling short. "I still cannot point to specific successes of our efforts here on terrorist financing," he said.

Copyright © 2006 Agence France Presse

###

 Printer Friendly Version  E-Mail This Article

FAIR USE NOTICE

This site contains copyrighted material the use of which has not always been specifically authorized by the copyright owner. We are making such material available in our efforts to advance understanding of environmental, political, human rights, economic, democracy, scientific, and social justice issues, etc. We believe this constitutes a 'fair use' of any such copyrighted material as provided for in section 107 of the US Copyright Law. In accordance with Title 17 U.S.C. Section 107, the material on this site is distributed without profit to those who have expressed a prior interest in receiving the included information for research and educational purposes. For more information go to: <http://www.law.cornell.edu/uscode/17/107.shtml>. If you wish to use copyrighted material from this site for purposes of your own that go beyond 'fair use', you must obtain permission from the copyright owner.

Common Dreams [NewsCenter](#)

A non-profit news service providing breaking news & views for the progressive community.

[Home](#) | [Newswire](#) | [Contacting Us](#) | [About Us](#) | [Donate](#) | [Sign-Up](#) | [Archives](#)

© Copyrighted 1997-2006
www.commondreams.org