The Changing Landscape of Tax Audits and Investigations

By
Bryan C. Skarlatos*

Bryan Skarlatos looks at how the September 11, 2001, terrorist attacks have increased the level of attention to financial transactions, thereby leading government agents to find tax evasion schemes.

September 11, 2001, changed the world in many ways, both large and small. Perhaps one of the least expected changes is the way in which tax audits and investigations will be conducted in the future.

How could a terrorist attack affect tax audits and investigations? For the most part, there is no direct connection between terrorism and taxes. However, there is a connection between taxes and financial transactions, and a similar connection between financial transactions and terrorism. Terrorism, by its very nature, is based on surprise and unpredictability. In the aftermath of September 11, governmental investigators have learned that, aside from monitoring the movements and communications of suspected terrorists, one of the most effective ways to track and anticipate terrorist activity is to monitor financial transactions for signs of unusual or suspicious flows of money.

As an example, imagine for a moment a law enforcement agent, highly sensitized to possible terrorist activity, reviewing wire transfers for signs of large transactions with offshore bank accounts. The agent notices a $3 million transfer wire transfer from an individual's New York account to an account in the Bahamas. Tracking the flow of money backward, the agent discovers that the day before the money was transferred to the Bahamian account, the same money was transferred by wire to the individual's New York account from a corporate account in Pittsburgh, Pennsylvania. Her suspicions peaked, the agent expands her review of the Pittsburgh and New York accounts and notices two other similar back-to-back wire transfers with the money ending up offshore.

The agent reports her findings to criminal investigators who interview the individual with the New York bank account. The investigators quickly learn that there is a

Bryan C. Skarlatos is a partner with Kostelanetz & Fink, LLP, in New York City. He focuses his practice on civil and criminal tax controversies and fraud-oriented commercial litigation.

©2003 B.C. Skarlatos

seemingly innocent explanation for the wire transfers and that no terrorist activity is involved. The New York individual is an art broker who arranged for the sale of three expensive paintings to a wealthy executive of the Pittsburgh corporation. The executive paid for the art by transferring money from the corporation's account to the broker's account, and, after subtracting his commission, the broker transferred the balance of the payment to the foreign owner of the paintings who operated a legitimate art business through a Bahamian bank account.

The story doesn't end there, however. After interviewing the New York art broker and reviewing documents he supplied, the investigators notice that no provision has been made for the payment of sales tax at any stage of the transactions. Picking up on this new line of inquiry, the investigators begin reviewing the executive's art-buying habits. A few months later, the investigators strike gold when they interview another art broker who admits that she arranged for certain pieces of art to be delivered to the executive's New York apartment even though the invoices falsely indicated that the art was shipped to locations outside of New York thereby allowing the executive to evade payment of millions of dollars in New York State sales tax on the art purchases.

Of course, this is not just a hypothetical fact pattern. It is the real-life story of the Denis Kozlowski/Tyco International, Ltd. investigation. Although Mr. Kozlowski is being prosecuted for evasion of state sales tax, there is no doubt that the investigation has raised many federal tax issues for Mr. Kozlowski as well, the most obvious of which is the use of corporate funds to purchase personal artwork. And it all started when a law enforcement agent noticed some unusual wire transfer activity.

Thus, as was the situation with organized crime figures like Al Capone and John Gotti, prosecutors will not hesitate to use more traditional tax crimes to prosecute terrorism-related cases.

Law Enforcement Agents Have Become More Sensitive to Taxpayers' Financial Transactions

September 11 has changed the way in which law enforcement agencies think about financial transactions. In the current climate, there is a greater sensitivity to the connection between the flow of money and illegal activity, and that is bad news for taxpayers who would prefer to shield their financial transactions from governmental inquiry. Tax audits and investigations traditionally have started from several different sources such as random audits, specific audit projects, examinations of related taxpayers, internal record matching programs, reviews of public records and tips from private parties. Now that law enforcement agents from various government agencies have learned to investigate financial transactions as a possible indicator of criminal activity including terrorism, money laundering and tax evasion, there is no doubt that such investigations will trigger tax cases and will become a major source of tax audits and investigations in the future.

Sometimes the evolution from a nontax investigation into a tax prosecution is purely coincidental. In many situations, however, it is no accident that what starts as a terrorism, money laundering, organized crime or drug investigation ends up as a civil or criminal tax case. Skilled government agents are always on the lookout for possible tax violations because they understand that tax violations are often the easiest way to pursue other crimes, such as terrorism, that can be more difficult to prove. For example, an activist suspected of raising money for terrorists recently was indicted in Chicago on charges that included lying to the IRS about the finances of his charitable organization.[1] In another investigation in Virginia, prosecutors believe that a charitable organization suspected of raising money for terrorism mislead the IRS about the use of funds raised from donors.[2] Thus, as was the situation with organized crime figures like Al Capone and John Gotti, prosecutors will not hesitate to use more traditional tax crimes to prosecute terrorism-related cases.

At the same time that law enforcement agencies have become more sensitive to financial transactions, Congress has ensured that they will have plenty of financial information to review by enacting new laws designed to increase the amount of financial information that is collected by businesses and reported to the government. Nearly

30 years ago, beginning with the Bank Secrecy Act,[3] Congress started building a statutory scheme that requires individuals and businesses to create and maintain records of all kinds of financial transactions and, in many cases, to report suspicious transactions to law enforcement officers. The stated purpose of this statutory scheme is "to require certain reports or records where they have a high degree of usefulness in criminal, tax or regulatory investigations or proceedings."[4] Thus, the very purpose of these information gathering, record keeping and reporting requirements is to assist law enforcement agencies in conducting tax audits and investigations as well as other regulatory and criminal proceedings.

The Treasury Extends the Reach of the Information Gathering and Record Keeping Requirements

Even before September 11, financial institutions, businesses and taxpayers were obligated to file several different types of reports regarding certain financial transactions and suspicious activity. For example, financial institutions must file currency transaction reports reporting currency transactions (deposits or withdraws) in excess of $10,000[5] and they must file Suspicious Activity Reports detailing any suspicious activity that comes to their attention.[6] Individuals who transport more than $10,000 of currency or monetary instruments into or out of the country have to file a Currency and Monetary Instrument Report with the Customs Service.[7] Any business that receives more than $10,000 of cash in a trade or business must file a Form 8300 with the IRS.[8] In addition, taxpayers are required to file forms with the Treasury reporting any interest they may have in a foreign bank or financial account with a value of more than $10,000.[9] While the government has not always been adept at organizing and applying all the information generated by these reports, the information in these reports has created a fertile source of leads for investigators and pitfalls for taxpayers involved in tax audits and investigations.

In the wake of September 11, Congress was anxious to create new sources of financial information for investigators to review in the hope that more information in the hands of government agents will assist in the detection of terrorist activity before it occurs. On October 26, 2001, the President signed into law the Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism (USA PATRIOT) Act of 2001 ("the Patriot Act").[10] While the Patriot Act does not specifically address tax audits and investigations, several provisions of the Patriot Act amend the Bank Secrecy Act to expand the scope of the information gathering, record keeping and reporting requirements imposed on businesses. These new laws will generate mountains of information about taxpayers' financial transactions and, once the government learns to organize, absorb and apply all of this information, law enforcement agents will have easy access to nearly every detail of taxpayers' financial lives.

The new requirements imposed by the Bank Secrecy Act, as amended by the Patriot Act, are imposed primarily on "financial institutions." The key to understanding the reach of these new laws lies in the definition of what constitutes a "financial institution." The Bank Secrecy Act defines the term "financial institution" to include not only institutions such as federally insured banks, commercial banks and private banks, but also broker dealers, currency exchangers, entities that accept or cash traveler's checks or money orders, credit card companies, insurance companies, jewelry dealers, pawnbrokers, loan companies, travel agencies, licensed money senders, businesses engaged in vehicle sales (*e.g.*, cars, planes and boats), persons involved in real estate closings and settlements (possibly even lawyers and accountants), the U.S. Postal Service, certain casinos and *any other businesses that the Secretary of the Treasury designates* by regulation.[11] Thus, Congress has created a legal framework in which several enumerated small businesses, and any other business designated by the Treasury, could be required to collect and report information about their customers and their transactions to government agencies.

Despite this extremely broad definition of what constitutes a "financial institution," Congress has allowed the Treasury to narrow the reach of these laws by issuing regulations expressly defining what types of businesses are subject to various record keeping and reporting requirements. In the past, the Treasury has exempted most businesses, other than banks, from the information gathering, record keeping and reporting requirements. However, in the wake of September 11, the Treasury acted quickly to begin expanding the reach of these laws. Now, for the first time ever, businesses such as broker

dealers, mutual funds, unregistered investment companies (*e.g.*, hedge funds), credit card companies, jewelry dealers and possibly even travel agents and car dealerships will be required to collect and report information about their customers and their transactions to the government.

The Patriot Act itself created two new types of information gathering and record keeping requirements that will affect domestic businesses: the "Know Your Customer" rules and the "Anti-Money Laundering Program" rules. Act Sec. 326 of the Patriot Act establishes Know Your Customer rules, which require banks, broker dealers, mutual funds and futures commodities merchants to collect and maintain information regarding the identity of any customer who wishes to open an account. The Treasury has issued several notices of proposed rulemaking under this section, laying out the specific types of information that must be collected by each type of financial institution.

Few people realize that the Patriot Act and recent Treasury rules have expanded significantly the amount of information that must be collected and maintained by businesses about their customers' financial lives.

For example, banks must have a written Customer Identification Program approved by the board of directors and tailored to the bank's size, location and type of business. At a minimum, the program must require the bank to gather the following information about its customers: name, date of birth, mailing address, primary place of business (for nonindividual customers) and identifying numbers, such as taxpayer identification numbers and (for foreign customers) passport and visa numbers. The bank's program must contain procedures describing how the bank will verify this information using documentary and nondocumentary evidence, and how the bank will respond when such evidence is not available (*i.e.*, the process by which nonverifiable customers' accounts will be closed). Furthermore, the bank's program must describe its record keeping practices and provide that the bank must keep these records for at least five years after the account is closed. Finally, the bank must notify its customers of the identification verification efforts, and its program must contain provisions that the bank will compare this information with any list of suspected terrorists provided it by a federal agency.[12]

Separate notices of propose rulemaking were issued for broker-dealers,[13] mutual funds[14] and futures commission merchants and introducing brokers.[15] All of the notices impose substantially the same information gathering and record keeping requirements. These Know Your Customer rules are designed to ensure that the types of financial institutions described above are sure about the identity of the people and entities with whom they do business. At the same time, this new information will provide a database from which law enforcement agents will be able to learn about nearly all of the financial accounts of a particular taxpayer.

The second main record keeping requirement for domestic businesses created by the Patriot Act is set forth in Act Sec. 352, which obligates financial institutions to establish Anti-Money Laundering Programs. The list of businesses that must establish Anti-Money Laundering Programs is broader than the list of businesses subject to the Know Your Customer rules. To date, the Treasury has issued specific rules covering banks, money service businesses, mutual funds, credit card companies, unregistered investment companies, insurance companies and dealers in precious metals and stones. In addition, the Treasury has solicited comments on how these new rules should be applied to travel agents and vehicle dealers (*i.e.*, sellers of automobiles, boats and airplanes).[16]

The purpose of an Anti-Money Laundering Program is to detect and prevent financial transactions connected with illegal activity. The Anti-Money Laundering Programs envisioned by Congress must include policies and procedures, including training and audit programs, to achieve this purpose. The Treasury has issued a series of notices of proposed rules under this section that are similar to the Know Your Customers rules and require businesses to collect and verify information regarding customers' identities. The new rules also require businesses to respond to governmental requests for information.[17] Separate notices with specific requirements have been issued for particular industries. For example, credit card companies, unregistered investment companies, insurance companies and,

continued on page 51

finally codified by legislation. It appears that the introduction of recent dispute resolution tools may have an adverse impact on perceived or actual independence. I believe the Appeals organization must seize the moment and guard its hard-earned reputation for making determinations based solely on its assessment of the litigation hazards. True independence can only be accomplished by eliminating the barriers, real or perceived, to an independent assessment of the merits of each particular taxpayer's case consistent with the Appeals mission.

ENDNOTES

1. Notice 2001-67, 2001-2 CB 544.
2. Rev. Proc. 2000-43, 2000-2 CB 404.
3. David B. Robison, *Robison Statement on Tax Shelter Settlement Initiative*, 2002 TNT 194-34 (Oct. 7, 2002).
4. Rev. Proc. 2002-44, IRB 2002-26, 10.
5. Announcement 2002-60, IRB 2002-26, 28.
6. IRM 8.1 (Appeals).
7. Announcement 2002-96, IRB 2002-43, 756.
8. Announcement 2002-97, IRB 2002-43, 757.
9. Rev. Proc. 2002-67, IRB 2002-43, 733.
10. Announcement 2002-110, IRB 2002-50.
11. CDO No. 247 (Rev. 1), 1996-1CB 356.
12. Rev. Proc. 79-34, 1979-2 CB 498.
13. Vicky Tsilas, *IRS Is Centralizing Management of Appeals Function, Richardson Says*, 96 TNT 242-2 (Dec. 13, 1996).
14. Act Sec. 1001(a)(3) of the IRS Restructuring and Reform Act of 1998 (P.L. 105-206).
15. *Id.*, Act Sec. 1001(a)(4).
16. Code Sec. 7123(b)(2).
17. Announcement 2003-3, IRB 2003-4, 361.
18. B. John Williams, *Williams Statement on IRS's Shelter Resolution Initiative*, 2002 TNT 194-32 (Oct. 7, 2002).
19. *IRS Issues FAQs on Contingent Liability Settlement Initiative*, 2003 TNT 12-6 (Jan. 17, 2003).
20. *Taxpayers to Contact "Lead Executives" to Have Say in Shelter Transaction Resolution*, 2003 TNT 28-3 (Feb. 11, 2003).
21. Rev. Proc. 99-28, 1999-2 CB 109.

Changing Landscape

continued from page 26

eventually, dealers in precious metals and stones all will have to create programs to prevent their systems or products from being used to facilitate money laundering or terrorist activities.[18] While the details of such programs are left to the discretion of particular businesses, to be effective, such programs necessarily will have to collect information about the identity of customers using or purchasing the businesses' systems or products and how or why those systems or products are being used. Again, once this information is collected, it will serve as a database for law enforcement agents to track the financial lives of taxpayers.

By expanding these information gathering and record keeping requirements to mutual funds, unregistered investment companies, credit card and insurance companies, jewelry dealers, travel agents and vehicle dealers, Congress and the Treasury have changed significantly the rules of the game. Prior to September 11, many people understood that the government was aware of certain business and bank transactions involving large amounts of cash. However, most Americans would be shocked to learn that businesses such as credit card companies, jewelry dealers, travel agents and car dealers are required to keep files on their customers and provide them to government agents on demand.

Expanded Suspicious Activity Reporting and Information Sharing Rules

What are the businesses supposed to do with all the information collected about their customers? In most cases, the data is simply kept in files, awaiting a formal or informal request from a government agent. However, certain financial institutions also have an obligation to file reports with the government disclosing any activity that appears to be suspicious. Prior to September 11, banks and money services businesses, including check cashers and issuers, sellers and redeemers of money orders and traveler's checks were required to file Suspicious Activity Reports (SARs), reporting any suspicious transaction relevant to a possible violation of law or regulation if the transaction involves at least $5,000 in funds or other assets. Over the last 18 months, the Treasury has expanded the list of businesses required to file SARs to include casinos and "card clubs,"[19] broker-dealers,[20] currency dealers and exchangers,[21] and mutual funds.[22]

In addition to expanding the list of business required to file SARs, the Patriot Act directed the Treasury to adopt regulations to encourage cooperation and information sharing between financial institutions, regulatory authorities and law enforcement agencies.[23] In response, the Treasury recently issued rules pursuant to which financial institutions may share information regarding individuals' accounts and transactions with other institutions for the purpose of identifying and reporting on money laundering and terrorism, or for the purpose of deciding whether to open an account or engage in a transaction. If both institutions have given notice to the Treasury of their intent to participate in such sharing and if both institutions have taken steps to ensure that the information shared is used for the purposes of this rule, then the institutions are exempt from liability for sharing such information.[24] In addition, any federal law enforcement agency may request

information regarding a financial institution's accounts of, or transactions with, named individuals if the law enforcement agency has reasonably credible evidence that the individual is involved in terrorism or money laundering.[25] To complement these new information-sharing procedures, Congress has directed the Treasury to create a highly secure computer network to allow for online sharing of information and filing of required reports.[26] The intent of this legislation is to make the above-described financial information more accessible to law enforcement agencies by harnessing the power of computers and the Internet.

Conclusion

Few people realize that the Patriot Act and recent Treasury rules have expanded significantly the amount of information that must be collected and maintained by businesses about their customers' financial lives. At the same time, the Treasury has increased the number and types of businesses required to report suspicious activity and has created new rules to facilitate the sharing of information between financial institutions and with the government. The consequences of all this information being gathered, shared among financial institutions and reported to the government are far-reaching indeed, especially in the current environment in which government agents have become increasingly sensitive to unusual financial transactions as possible evidence of illegal activity. As this information accumulates over the years, and as the government's ability to organize and use this information increases, we will be living in a brave new world in which big brother has access to nearly all aspects of taxpayers' financial lives. Aside from the obvious privacy concerns, the implications for tax audits and investigations are enormous.

ENDNOTES

* Andrew Kirk Susong assisted in the preparation of this article.
1 *U.S. Tries Al Capone Tax Charges in Some Terror-Financing Cases,* WALL ST. J., Oct. 10, 2002.
2 *Id.*
3 31 USC §5311, *et seq.*
4 31 USC §5311.
5 31 USC §5313(a).
6 31 USC §5318(g).
7 31 USC §5316(a).
8 Code Sec. 6050I.
9 31 CFR §103.24.
10 Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism Act of 2001 (P.L. 107-56).
11 31 USC §5312(a)(2), as amended by the Patriot Act.
12 *See* 67 FR 48290 (July 23, 2002) (to be codified at 31 CFR §103.121). An identical proposed rule was published elsewhere by FinCEN alone, without the aegis of the federal bank regulators, applicable to those banks not otherwise subject to federal bank regulation. *See* 67 FR 48299 (July 23, 2002).
13 *See* 67 FR 48306 (July 23, 2002) (to be codified at 31 CFR §130.122).
14 *See* 67 FR 48318 (July 23, 2002) (to be codified at 31 CFR §130.131).
15 *See* 67 FR 48328 (July 23, 2002) (to be codified at 31 CFR §103.123).
16 *See* 67 FR 8571 (Feb. 24, 2003); 67 FR 8568 (Feb. 24, 2003).
17 *See* 67 FR 21114 (Apr. 29, 2002) (to be codified at 31 CFR §103.125). A similar interim final rule was promulgated for mutual funds. *See* 67 FR 21117 (Apr. 29, 2002) (to be codified at 31 CFR §103.130).
18 *See* 67 FR 21121 (Apr. 29, 2002) (to be codified at 31 CFR §103.135); 67 FR 60617 (Sept. 26, 2002) (to be codified at 31 CFR §130.132); 67 FR 60625 (Sept. 26, 2002) (to be codified at 31 CFR §103.137); and 67 FR 8480 (Feb. 21, 2003) (to be codified at 31 CFR §103.140).
19 *See* 67 FR 60722 (Sept. 26, 2002) (adding 31 CFR §103.21).
20 See 67 FR 48488 (July 24, 2002).
21 *See* 68 FR 6613 (Feb. 10, 2003) (amending 31 CFR §103.20(a)(1)).
22 *See* 68 FR 2716 (Jan. 21, 2003) (to be codified at 31 CFR §103.15).
23 Act Sec. 314 of P.L. 107-56.
24 *See* 31 CFR §103.110.
25 *See* 31 CFR §103.100.
26 Act Sec. 362 of P.L. 107-56.

IRS Customer Service

continued from page 29

and the Service may view themselves in a significantly more adversarial role if they perceive that the Service is unfairly using its regulatory authority over them to take actions contrary to their clients' interests."

Chicago attorney and ABA Tax Section Liaison to IRS Wage & Investment, Robert E. McKenzie, believes this new level of inquiry by the PPS staff is "a wrong-headed policy that thwarts problem solving." He continues:

> If we wanted demands for levy information we would call ACS or collection. Given the current policy, I recommend that practitioners refuse to deal with PPS. This change in approach suggests they do not recognize the practitioner's role in resolving tax delinquencies. Under the current policy an attempt to secure information could result in disclosure of information the Service will use to harm the practitioner's client.

ENDNOTES

1 IRM sub-subsection 5.19.1.3.3.3. Date document last amended: Oct. 1, 2001. Obtain and Verify Levy Sources
"(1) You must attempt to secure at least one potential levy source on accounts above deferral (see Section 1.3.3.2 above) when speaking to the taxpayer.
EXCEPTION — If account is in status 22 and the balance is above $100, secure levy source.
(2) Obtain the name, address, and ZIP code on the following potential levy sources:
- Taxpayer's employer
- Taxpayer's bank
- Taxpayer's credit union
- Establishments/businesses for which the taxpayer provides self-employed contract services."