Money Laundering

In This Issue

September 2007
Volume 55
Number 5

United States
Department of Justice
Executive Office for
United States Attorneys
Washington, DC
20530

Kenneth E. Melson
Director

Contributors' opinions and statements should not be considered an endorsement by EOUSA for any policy, program, or service.

The United States Attorneys' Bulletin is published pursuant to 28 CFR § 0.22(b).

The United States Attorneys' Bulletin is published bimonthly by the Executive Office for United States Attorneys, Office of Legal Education, 1620 Pendleton Street, Columbia, South Carolina 29201.

Managing Editor
Jim Donovan

Program Manager
Nancy Bowman

Internet Address
www.usdoj.gov/usao/reading_room/foiamanuals.html

Send article submissions and address changes to Program Manager, United States Attorneys' Bulletin,
National Advocacy Center,
Office of Legal Education,
1620 Pendleton Street,
Columbia, SC 29201.

Introduction

Richard Weber
Chief, Asset Forfeiture and Money Laundering Section
Criminal Division

Money laundering constitutes a significant threat to the safety of our communities, the integrity of our financial institutions, and our national security. In order to effectively address this serious threat, the best efforts to apply and coordinate all of the available resources of the federal government, along with those of state and local authorities, as well as our foreign counterparts, must be used. The United States Department of Justice is fully committed to using the money laundering and asset forfeiture statutes to the fullest extent possible. They will be used to identify, investigate, and prosecute those who launder the illegal proceeds of terrorists, drug traffickers, fraud perpetrators, organized crime organizations, and other criminals, and to seize and forfeit their ill-gotten assets.

In recent years, crime has become increasingly international in scope, and the financial aspects of crime have become more complex. This is due to the rapid advances in technology and the globalization of the financial services industry. Modern financial systems permit criminals to transfer millions of dollars instantly though personal computers and satellite dishes. Money is laundered through currency exchange houses, stock brokerage houses, gold dealers, casinos, automobile dealerships, insurance companies, trading companies, and other sophisticated systems. Private banking facilities, offshore banking, shell corporations, free trade zones, wire systems, and trade financing all have the ability to mask illegal activities. The criminal's choice of money laundering vehicles is limited only by his or her creativity. Ultimately, this laundered money flows into global financial systems where it can undermine national economies and currencies.

Organized criminal groups transcend national borders and extend their influence to areas of the world far-removed from their countries of origin. The gradual erosion of border controls in the countries of Europe not only contributes to the free flow of trade and commerce, but also increases the threat of transborder financial crimes. This internationalization of crime makes the sharing, collating, and analysis of information, among and within governments, essential.

Organized criminals are motivated by one thing—profit. Greed drives the criminal. Huge sums of money are generated through drug trafficking, arms smuggling, white collar crime, human trafficking, terrorism, and corruption. The end result is that organized crime moves billions of illegally-gained dollars into our nation's legitimate financial systems. The success of organized crime is based upon its ability to launder money.

The challenges facing law enforcement in this environment make it necessary for investigators and prosecutors to have all the legal and regulatory tools, as well as international legal assistance mechanisms available to them, to keep up with, and ahead of, those who launder the proceeds of crime. To effectively combat such criminal activity, law enforcement must have the means that are at least as sophisticated, if not more so, than the criminals.

The money laundering statutes Congress provided, both in the Bank Secrecy Act and the Criminal Code, are major weapons in the war against the laundering of drug trafficking proceeds and other serious crimes. These weapons gut the economic base that these criminals need to operate and stops them from continuing business as usual, which is integral to the fight against terrorism. It also prevents replacement of members who have been incarcerated. Another tangential benefit is the deterrence of crime. Greed is one of the primary reasons for criminal activity. Asset forfeiture removes this incentive by denying criminals the assets illegally acquired. Not only will they go to jail, but they will not realize any economic gain from the crime.

Investigating and prosecuting money laundering and forfeiting criminal assets can be a long, arduous, and complex process. It is critical to bear in mind, however, that it is more than a bloodless exercise in accounting. When the crime of money laundering is fought, organized crime is fought. The fight against money laundering accomplishes the following goals, among many others.

- Keeps drugs out of playgrounds and away from children.
- Safeguards the human dignity of women and children trafficked into forced labor and prostitution.
- Most importantly, keeps funding out of the hands of terrorists.

The Asset Forfeiture and Money Laundering Section (AFMLS) releases several publications, including the monthly *Asset Forfeiture Quick Release* (new forfeiture case law) and the bi-monthly *Asset Forfeiture News.* This edition of the *United States Attorneys' Bulletin* supplements those publications and is intended to provide an overview of the money laundering statutes and a survey of some of the tools that can be used in financial investigations. A future edition of the *Bulletin* will focus on asset forfeiture and provide a series of articles on that topic.

The articles in this edition of the *Bulletin* cover several topics, including those listed below.

- An overview of the statutes used to combat money laundering, including the primary money laundering statutes (18 U.S.C. §§ 1956 and 1957), the Bulk Cash Smuggling statute (31 U.S.C. § 5332), and the Unlicensed Money Remitting Statute (18 U.S.C. § 1960).
- Money laundering trends and techniques.
- Tools to use in financial investigations.
- The use and disclosure of Suspicious Activity Reports in investigations.
- Criminal enforcement actions against banks for the failure to file Suspicious Activity Reports or to have effective Anti-Money Laundering programs.

The AFMLS is committed to using the money laundering statutes to the fullest extent possible and stands ready to give whatever support and advice is needed in prosecuting money laundering and asset forfeiture cases.❖

ABOUT THE AUTHOR

❑**Richard Weber** has served as the Chief of the Asset Forfeiture and Money Laundering Section since March 2005. Prior to that, he was an Assistant United States Attorney in the Eastern District of New York, serving as Deputy Chief of the Civil Division and Chief of the Asset Forfeiture Unit. Rich first joined the Department under the Attorney General's Honor Program. His expertise in asset forfeiture and money laundering has developed from prosecuting over 100 complex international and domestic money laundering and asset forfeiture cases. Among many others, he prosecuted *U.S. v. Blarek/Pellecchia*, 166 F.3d 1202 (2d Cir. 1998) (interior decorators were convicted of laundering millions of dollars of drug proceeds for the leader of the Cali cartel and forfeited $7 million dollars); *U.S. v. Jordan Belfort and Daniel Porush*, 98-cr-00859-JG (E.D. N.Y. Oct. 14, 2003) (where an international securities fraud money laundering investigation resulted in the forfeiture of $15 million dollars); and *U.S. v. Palm View Corp*, 99-cr-00702-ILG (E.D. N.Y. July 21, 2000) (which involved gambling proceeds and the forfeiture of $6 million dollars).✠

Suspicious Activity Reports Disclosure and Protection

Lester Joseph
Principal Deputy Chief
Asset Forfeiture and Money Laundering Section
Criminal Division

I. Introduction

Suspicious Activity Reports (SARs) have become one of law enforcement's most valuable tools for detecting and investigating criminal activity. Banks have been notifying law enforcement of suspected criminal activity for many years, either by submitting Criminal

Referral Forms or by checking the "suspicious" box on the old Currency Transaction Reports (CTRs). The modern SAR program came into effect on April 1, 1996, when the Treasury Department regulations requiring banks to file SARs became effective. *See* 31 C.F.R. § 103.18. Other types of financial institutions have subsequently been required to file SARs as of the dates shown in Figure 1. As of 2006, the financial institutions shown in Figure 2 have filed more than four million SARs.

The SAR system is designed to assist the law enforcement community by requiring financial institutions to report transactions that are indicative of possible violations of law or regulation. The required threshold for filing is easily triggered, simply by suspicions, not proof, of illegal activity. The information contained in SARs constitutes raw allegations of the most sensitive kind, precisely because the reported "suspicions" are unsubstantiated and unproven.

Financial institutions file SARs with the expectation that they will be accorded sensitive treatment. Unnecessary disclosure of SARs could frustrate that expectation and have a chilling effect on both the quantity and the quality of future SAR filings. Moreover, SARs may contain information concerning the methods by which an institution learned of or uncovered suspicious activity, possibly allowing other potential wrongdoers to take action to avoid those methods of detection. Therefore, it is essential that law enforcement agencies and prosecutors take measures to ensure that the existence of a SAR or its contents are not disclosed unless absolutely necessary or required by law.

II. Protection and disclosure by financial institutions

Financial institutions have a significant interest in protecting SARs from disclosure. Institutions are generally reluctant to publicize the fact that they have filed SARs on their customers, and certainly do not want their customers to know that they have reported their activity to the government. This reluctance is based upon both business and safety concerns. Institutions know that their customers would not be pleased to have their suspicious transactions reported to the government, and are also concerned about retaliation from customers whose transactions have been reported. This is especially true in small communities where it would be obvious which institution or employee filed the SAR. However, to ensure that complicit or corrupt bank officers do not tip off a customer concerning the filing of a SAR, 31 U.S.C. § 5318(g) includes the following provision.

> (2) NOTIFICATION PROHIBITED.--
>
> (A) IN GENERAL.--If a financial institution or any director, officer, employee, or agent of any financial institution, voluntarily or pursuant to this section or any other authority, reports a suspicious transaction to a government agency--
>
> (i) the financial institution, director, officer, employee, or agent may not notify any person involved in the transaction that the transaction has been reported....

The SAR statutory scheme also contains a "safe harbor" provision that protects financial institutions from civil liability resulting from the reporting of suspicious transactions.

> (A) IN GENERAL.--Any financial institution that makes a voluntary disclosure of any possible violation of law or regulation to a government agency or makes a disclosure pursuant to this subsection or any other authority, and any director, officer, employee, or agent of such institution who makes, or requires another to make any such disclosure, shall not be liable to any person under any law or regulation of the United States, any constitution, law, or regulation of any State or political subdivision of any State, or under any contract or other legally enforceable agreement (including any arbitration agreement), for such disclosure or for any failure to provide notice of such disclosure to the person who is the subject of such disclosure or any other person identified in the disclosure.

31 U.S.C. § 5318(g)(3).

The major issue that courts have disagreed on is whether the safe harbor provision is an unqualified privilege or whether there is a good faith belief requirement in the language of the statute. In *Lopez v. First Union Nat'l Bank*, 129 F.3d 1186 (11th Cir. 1997), an account holder filed a lawsuit against the bank alleging *inter alia* violations of the Right to Financial Privacy Act after the bank notified law enforcement that there were unusual movements of money in certain accounts at the bank. The court dismissed the

complaint based on its conclusion that § 5318(g) immunized the bank from liability. The Eleventh Circuit reversed the dismissal, finding that "there must be some good faith basis for believing [that] there is a nexus between the suspicion of illegal activity and the account or accounts from which information was disclosed." *Id.* at 1195. The court was concerned because the bank disclosed information about 1,100 accounts based on "unusual movements of money at the bank," but may not have had a good faith basis for believing that there was suspicious activity in each of the 1,100 accounts. *Id.*

The Second Circuit ruled differently two years later in *Lee v. Bankers Trust Co.*, 166 F.3d 540 (2d Cir. 1999), holding that there is no good faith requirement in §5318(g). *Lee*, a former managing director for Bankers Trust, brought an action alleging that the bank defamed him through its conduct in investigating wrongdoing with respect to the transfer of unclaimed accounts and through the alleged filing of a SAR after he was asked to resign. In affirming the District Court's granting of a motion to dismiss, the Second Circuit stated, "The plain language of the safe harbor provision describes an unqualified privilege, never mentioning good faith or any suggestive analogue thereof." *Id.* at 544. The court also noted that a good faith requirement made no sense because, if the bank sought summary judgment, it would have to establish that the statements in the SAR were made in good faith, but it would be prohibited by law both from disclosing the filing or the contents of a SAR. Further, the court noted that an earlier draft of the safe harbor provision included an explicit good faith requirement, but that the requirement was not included in the bill that was finally enacted. *Id.* Note, however, that one state court has ruled that a bank may lose its safe harbor protection if a SAR is filed maliciously. *See Bank of Eureka Springs v. Evans*, 109 S.W.3d 672 (Ark. 2003).

In addition to prohibiting institutions from disclosing SARs to persons involved in a reported transaction and protecting financial institutions from civil liability resulting from filing SARs, FinCEN has issued regulations to prevent SARs from being disclosed during the course of litigation:

> (e) *Confidentiality of reports; limitation of liability....* [A]ny person subpoenaed or otherwise requested to disclose a SAR or the information contained in a SAR, except where such disclosure is requested by FinCEN or an appropriate law enforcement or bank supervisory agency, shall decline to produce the SAR or to provide any information that would disclose that a SAR has been prepared or filed, citing this paragraph (e) and 31 U.S.C. 5318(g)(2), and shall notify FinCEN of any such request and its response thereto.

31 C.F.R § 103.18(e). The Federal Reserve Board (12 C.F.R. § 208.62(j) (2006)), the Office of Thrift Supervision (12 C.F.R. § 563.180(d)(12) (2005)), and the Office of the Comptroller of the Currency (12 C.F.R. § 21.11(k)) have issued essentially identical regulations that apply specifically to the institutions under their respective jurisdictions. SARs have been sought by litigants in a variety of civil cases. In many of these cases, the government has intervened or filed briefs to prevent the disclosure of the SARs, and courts have generally been very supportive of the government's efforts to protect SARs from disclosure.

Courts have noted that the disclosure of a SAR could compromise an ongoing law enforcement investigation, provide information to a criminal wishing to evade detection, or reveal the methods by which banks are able to detect suspicious activity. *See, e.g., Cotton v. PrivateBank and Trust Co.,* 235 F. Supp. 2d 809, 815 (N.D. Ill. 2002); *Youngblood v. Comm'r,* 2000 WL 852449, *11-12 (C.D. Cal. Mar. 6, 2000). Courts have also observed that a bank may be reluctant to prepare a SAR if it believed that its cooperation may cause customers to retaliate. *See, e.g., Cotton,* 235 F. Supp. 2d at 815. Courts have also expressed concern that the disclosure of a SAR could harm the privacy interests of innocent people whose names may be mentioned. *See, e.g., id.*; *Weil v. Long Island Sav. Bank,* 195 F. Supp. 2d 383, 388 (E.D.N.Y.2001) ("the production of SARs by a bank in response to a subpoena would invariably increase the likelihood that the person involved in the transaction would discover or be notified that the SARs had been filed") (internal citations and quotations omitted); *Whitney Nat'l Bank v. Karam*, 306 F. Supp. 2d 678, 680-81 (S.D. Texas 2004).

For example, in *Weil v. Long Island Sav. Bank*, 195 F. Supp. 2d 383 (E.D.N.Y. 2001), borrowers sued the defendant bank in connection with a purported illegal kickback scheme involving the CEO. The plaintiffs moved to compel production of any SAR regarding the

CEO that had been filed with the Office of Thrift Supervision. The court held that 12 C.F.R. § 563.180(d)(12) "prohibit[ed] the disclosure of SARs or their content, even in the context of discovery in a civil lawsuit, and that the enabling legislation... [was] specific enough to support that purpose." The court further found that the statute created an unqualified discovery and evidentiary privilege that could not be waived by the reporting financial institution. *Id.* at 389.

In *Gregory v. Bank One, Indiana, N.A.,* 200 F. Supp. 2d 1000 (S.D. Ind. 2002), a bank that was a defendant in a civil lawsuit sought to disclose its own filing of a SAR. The plaintiff was a bank employee who asserted defamation and related claims arising from accusations of theft. The bank sought leave of court to submit, under seal for *in camera* review, any information that it might have reported pursuant to 31 U.S.C. § 5318(g)(2) in support of an affirmative safe harbor immunity defense. While the court initially granted the request, upon reconsideration, it vacated its order and returned the materials produced. The court explained.

> There is no provision in the Act or the Rule allowing a court-order exception to the unqualified privilege. [citation omitted] Thus, the Court is not authorized to order or to permit Bank One to make any disclosure, sealed or unsealed, of any information which is privileged under the Act or the Rule, whether in the form of a copy of an SAR or other report.... Quite the opposite: under the clear, unambiguous terms of the Act and the Rule, courts have an obligation to prevent disclosures of privileged information.

Id. at 1003.

Although the regulations issued by the federal regulators are broader in their prohibitions against disclosure of the existence or the content of a SAR than is the statute, the regulations have been held to be consistent and in harmony with the enabling statute. In *Cotton v. PrivateBank & Trust Co.,* 235 F. Supp. 2d 809 (N.D. Ill. 2002), during the course of civil litigation concerning an estate, *PrivateBank* sought the disclosure of certain SARs from CIBC World Market Corp (CIBC). PrivateBank argued that disclosure of the SARs by CIBC would not violate the statutory scheme because 31 U.S.C. § 5318(g) prohibits disclosure of a SAR only to any person involved in the transaction. PrivateBank contended that the regulations are inconsistent with the statute and, therefore, unenforceable. The court, citing *Gregory* and *Weil*, disagreed, and held that the regulations were consistent with the statute and should be enforced. *Id.* at 815.

III. Disclosure of supporting documents

Courts have, however, made a distinction between disclosure of SARs and disclosure of the supporting documents underlying the SAR. Under the regulations, the supporting documents underlying the SAR are not to be filed with the SAR, but are to be retained by the financial institution and treated as if they were filed with the SAR.

> (d) *Retention of records.* A bank shall maintain a copy of any SAR filed and the original or business record equivalent of any supporting documentation for a period of five years from the date of filing the SAR. Supporting documentation shall be identified, and maintained by the bank as such, and shall be deemed to have been filed with the SAR. A bank shall make all supporting documentation available to FinCEN and any appropriate law enforcement agencies or bank supervisory agencies upon request.

31 C.F.R. § 103.18(d).

The courts have generally held that the prohibition against a bank's disclosure of the existence or contents of a SAR does not apply to disclosure of any supporting documents. *See, e.g., Weil v. Long Island Sav. Bank,* 195 F. Supp. 2d 383, 389 (E.D.N.Y. 2001). "Nothing in the Act or regulations prohibits the disclosure of the underlying factual documents which may cause a bank to submit a SAR." *Cotton*, 235 F. Supp. 2d at 814. Furthermore, those underlying documents do not become confidential by reason of being attached or described in a SAR. For example, if a wire transfer of funds is described in a SAR as a suspicious activity, the wire transfer transaction remains subject to discovery. Therefore, the court in *Cotton* held that "the better approach prohibits disclosure of the SAR while making clear that the underlying transaction such as wire transfers, checks, deposits, etc., are disclosed as part of the normal discovery process." *Id.*

The *Cotton* court, however, distinguished between two types of supporting documents.

> The first category represents the factual documents which give rise to suspicious conduct. These are to be produced in the

> ordinary course of business because they are business records made in the ordinary course of business. The second category is documents representing drafts of SARs or other work product or privileged communications that relate to the SAR itself. These are not to be produced because they would disclose whether a SAR has been prepared or filed.

Id. at 815. In *United States v. Holihan*, 248 F. Supp. 2d 179 (W.D.N.Y. 2003), the defendant bank employee was charged with embezzlement. As part of her defense, the defendant served a subpoena on the bank for production of complete personnel files of the bank's investigator and other bank employees. The bank opposed the request of personnel files insofar as it would require the production of any SARs filed against any other bank employee working at the branch during the relevant time period. The court, citing *Gregory* and *Cotton*, ordered the disclosure of any supporting documents relating to a SAR in the personnel file of any relevant bank employee at the time of the embezzlement, provided that such documentation did not disclose either the existence or contents of a SAR. *Id*. at 187.

The case of *Union Bank of California v. Superior Court of Alameda County*, 130 Cal. App. 4th 378 (2005), further opined on the term "supporting documentation." Union Bank was sued by several investors who lost money in a Ponzi scheme. The fraud victims alleged that Union Bank was complicit in the operation of the scheme by allowing the perpetrators to set up a sham trust account that was used to transfer millions of dollars to offshore accounts. During the course of the litigation, the victims sought permission from the Office of the Comptroller of the Currency (OCC) to allow Union Bank to produce certain SARs it had filed during the relevant time frame. The OCC denied this request. During discovery, the victims learned that Union Bank had in place certain internal procedures and forms to identify, register, and describe what might constitute suspicious activity, particularly an internal form (Form 244) which is filled out by bank personnel to report suspicious activity. The victims requested the Forms 244 filed within the bank. The trial court ordered production of all such Forms 244, whereupon Union Bank filed a petition seeking a writ of mandate with the appellate court.

The California Appellate Court noted that "a draft SAR or internal memorandum prepared as part of a financial institution's process for complying with federal reporting requirements is generated for the specific purpose of fulfilling the institution's reporting obligation." The court found that "[t]hese types of documents fall within the scope of the SAR privilege because they may reveal the contents of a SAR and disclose whether a SAR has been prepared or filed." (Citation omitted). Unlike transactional documents, which are *evidence* of suspicious conduct, draft SARs and other internal memoranda or forms that are part of the process of filing SARs are created to *report* suspicious conduct. *Id.* at 391. This led the court to find that the Forms 244 are privileged documents that should not be disclosed.

> A bank's internal procedures may include the development and use of preliminary reports subject to various quality control checks before the bank prepares the final SAR that will be filed. Revealing these preliminary reports, the equivalent of draft SAR's would disclose whether a SAR had been prepared.

Id. at 392. Accordingly, the court held that the SAR privilege extends to documents prepared by a bank "for the purpose of investigating or drafting a possible SAR." *Id.* at 394.

IV. Disclosure by regulators

The *Union Bank* case referred to the fact that the fraud victims initially sought permission from the OCC to allow Union Bank to produce the SARs. The OCC's regulations prohibit financial institutions under its jurisdiction from disclosing SARs, and require that persons seeking disclosure of nonpublic documents, such as SARs, submit a request to the Director of the OCC's Litigation Division in Washington, D.C. *See* 12 C.F.R. § 4.34(a). The request must provide sufficient detail to apprise the OCC of the nature of the litigation, and the request must evidence that "the information is relevant to the purpose for which it is sought," that "other evidence reasonably suited to the requestor's needs is not available from any other source," and that "the need for the information outweighs the public interest considerations in maintaining the confidentiality of the OCC information and outweighs the burden on the OCC to produce the information." 12 C.F.R. § 4.33(a)(iii)(A)-(C). Finally, the OCC, alone, has discretion to deny these requests "based on its weighing of all appropriate factors

including the requestor's fulfilling of the requirements enumerated in § 4.33." 12 C.F.R. § 4.35(a).

Litigants, in some cases, have alleged that the OCC's denials of their requests for SAR information were arbitrary and capricious because they were not analyzed in conjunction with the regulatory requirements outlined above. One such complaint arose in the case of *Wuliger v. Office of the Comptroller of Currency*, 394 F. Supp. 2d 1009 (N.D. Ohio 2005). In *Wuliger*, an escrow agent used investors' money to fund several bank and brokerage accounts. After the investors suffered monetary losses, plaintiff was appointed as Receiver. In conjunction with his role, plaintiff submitted a request to the OCC for the release of SARs, all supporting documentation, and all correspondence, memos, or other documents pertaining to the investment of these funds. The OCC responded to the request by outlining the public policy in favor of maintaining SAR confidentiality, relying on the regulations requiring confidentiality, and citing to cases denying disclosure of SARs in the course of discovery proceedings. The court ruled that the OCC acted properly and that its decision could not be deemed arbitrary or capricious, even though the OCC did not conduct any analysis as to whether the plaintiff satisfied the burden established by its regulations. *Id.* at 1018.

The Eastern District of Louisiana, however, reached a contrary result in the case of *BizCapital Bus. & Indus. Dev. Corp. v. OCC,* 406 F. Supp. 2d 688 (E.D. La. 2005). *BizCapital* involved a SAR disclosure request and OCC response that were virtually identical to those analyzed in the *Wuliger* case. When the OCC denied BizCapital's request for disclosure, BizCapital filed suit in federal district court, seeking review of the OCC's final administrative decision. The district court granted BizCapital's cross-motion for summary judgment, rejecting the OCC's argument that it was absolutely prohibited from revealing SARs to third parties and determining that the OCC improperly failed to weigh the factors outlined in its own regulations prior to denying BizCapital's request. *Id*. at 692-93. The court ordered the OCC to submit any responsive SAR to the court for an *in camera* review so that a determination could be made regarding the appropriate extent of disclosure. *Id.* at 697-98. The OCC appealed the decision on the ground that the district court should have remanded the case to the OCC for further consideration, rather than ordering the disclosure of the SAR. The Fifth Circuit agreed and remanded the case to the district court. *BizCapital Bus. & Indus. Dev. Corp. v. OCC*, 467 F.3d 871 (5th Cir. 2006). This case leaves open the possibility that, at least in some cases, a civil litigant may be able to obtain disclosure of a SAR through a federal regulator during the course of civil litigation.

V. Disclosure by the government

Section 5318(g)(2)(A)(ii) addresses the disclosure of SARs by government employees.

> (ii) no officer or employee of the Federal Government or of any State, local, tribal or territorial government within the United States, who has any knowledge that such report was made may disclose to any person involved in the transaction that the transaction has been reported, other than as necessary to fulfill the official duties of such officer or employee.

While this provision further expresses the notion that SARs are confidential and should not be disclosed without authority or good cause, it does not begin to address the myriad of situations that prosecutors and investigators encounter during the course of a criminal investigation and prosecution. On its face, the restriction is limited to disclosure of the SAR or information related to the subject of the SAR, and excludes situations that are necessary to fulfill the employee's official duties. This leaves open numerous questions, such as the following.

- How should prosecutors deal with SARs during the course of carrying out their discovery obligations?
- How can investigators and prosecutors use SARs to support applications for search warrants and seizure warrants?
- How can investigators and prosecutors share SARs with other agents during the course of an investigation?

While there are no statutes or regulations that directly address these questions, the short answer is that every effort should be made by investigators and prosecutors to protect SARs from disclosure. As mentioned above, release of a SAR may jeopardize an ongoing investigation, alert criminals, disclose bank methods to detect suspicious activity, or alienate customers. *Cotton*

v. PrivateBank and Trust Co., 235 F. Supp. 2d 809, 815 (N.D. Ill. 2002).

Financial institutions are prohibited from disclosing SARs, and the financial regulators rigorously seek to protect SARs from being disclosed. It is only fair—and consistent with the spirit of the SAR program—that law enforcement does everything within its power to protect SARs from being disclosed. Therefore, the existence or contents of a SAR should only be disclosed when absolutely necessary, and only after there has been discussion with supervisors in the U.S. Attorneys' Offices or with the Criminal Division.

In 2003, the Department of Justice's (Department) Criminal Division issued guidance on the "Disclosure of Suspicious Activity Reports." This guidance is reproduced in Figure 3. The premise of the guidance is that "[l]aw enforcement agencies and prosecutors should consider SARs similar to confidential source information that, when further investigated, may produce evidence of criminal activity," and that, "[c]onsistent with the treatment accorded confidential source information, the existence of SARs... should not normally be disclosed to persons outside of the law enforcement community." The guidance also notes the distinction between SARs and the records underlying the SAR, and states, "[b]ecause the underlying documents prove the transaction, and the SAR does not, it should rarely be necessary to use a SAR in the prosecution's case."

In accordance with this premise, these general guidelines should be followed.

- SARs should not be referenced in affidavits for search warrants, Title IIIs, or seizure warrants. The underlying bank records should be sufficient to establish the basis for the search, seizure, or electronic surveillance.
- SARs should not be referenced in motions or responses to motions.
- SARs should not be referenced in indictments, informations, or any other charging documents.
- SARs should not be shown to subjects or witnesses during the course of interrogations.
- SARs should not be referenced in press releases.

There are certain situations where a prosecutor may have an obligation to disclose a SAR, or more likely, information included within a SAR, such as the following.

- [The SAR] contains exculpatory or potential impeachment information that a prosecutor is constitutionally obligated to disclose.
- [The SAR] is a document, or contains information, required to be disclosed under Rule 16 of the Federal Rules of Criminal Procedure or under the *Jencks* Act, 18 U.S.C. § 3500.

However, even in these situations, it should not be necessary to disclose the SAR, itself. The SAR is not the critical information. It is the information in the SAR that is relevant. Thus, if a SAR contains potential exculpatory information, the relevant information can, for example, be provided to defense counsel in a letter. In any case, prosecutors should not disclose a SAR, either in its entirety or in redacted form, before consulting with their supervisors, the Criminal Division, and FinCEN's Office of General Counsel. The disclosure of a SAR in any particular case can have consequences beyond the scope of that case.

VI. Sharing of SARs with other government personnel

The Department encourages the development of interagency SAR teams to review SARs and coordinate resulting investigations. There are restrictions, however, on the sharing of SARs and SAR information among law enforcement personnel, pursuant to applicable law and policy, aimed at protecting the integrity of these sensitive reports. There are significant privacy issues that arise from the use and disclosure of SARs.

FinCEN, in its role as the administrator of the Bank Secrecy Act (BSA), is the central point of dissemination of BSA information. In this role, FinCEN is responsible for ensuring that SARs are used appropriately and in a manner designed to respect the significant privacy interests that are at stake. In furtherance of this mission, in June 2004, FinCEN issued "Re-Dissemination Guidelines for Bank Secrecy Act Information" which established the procedures for the re-dissemination of BSA information by appropriate users of the data. These Re-Dissemination Guidelines were revised and reissued in December 2006.

The December 2006 Re-Dissemination Guidelines state that, subject to certain conditions, a federal, state, or local government agency may re-disseminate BSA information to another government agency in the following situations, without obtaining the approval of FinCEN.

• In support of a financial institution examination, law enforcement investigation, or prosecution.

• In the conduct of intelligence or counterintelligence activities, including analysis, to protect against international terrorism.

The conditions to this rule, in part, include the following.

- The disclosing federal, state, or local government agency must obtain a written acknowledgment of the receiving agency, reflecting its understanding that further dissemination of the BSA information is prohibited without the prior approval of FinCEN.
- The disclosing federal, state, or local government agency must ensure that each item of BSA information shared contains a specific warning statement which states that the information cannot be further released without prior approval from FinCEN.
- The disclosing federal, state, or local government agency must keep a record of each disclosure of BSA information.

The December 2006 Re-Dissemination Guidelines further state that BSA information can be re-disseminated, without first obtaining the approval of FinCEN, in the following specific situations.

- In limited circumstances, a federal prosecutor may disclose BSA information in the course of a judicial proceeding without first obtaining the approval of FinCEN. (See the discussion of the Department SAR Guidance, *supra*.)
- The federal bank supervisory agencies each have concurrent authority to re-disseminate a SAR that is filed with FinCEN by a bank or a banking organization.
- U.S. Customs and Border Protection and U.S. Immigration and Customs Enforcement have concurrent authority to re-disseminate a Currency and Monetary Instrument Report.

As the above is a brief synthesis of the Re-Dissemination Guidelines, it is imperative that the guidelines be reviewed prior to the sharing of any BSA information among law enforcement personnel. It is important that prosecutors and law enforcement agents be familiar with, and understand, these guidelines. The SAR Re-Dissemination Guidelines are available from FinCEN, or from the Asset Forfeiture and Money Laundering Section, or the Fraud Section, of the Criminal Division.

VII. Conclusion

SARs are one of the most valuable tools to proactive law enforcement. They allow the government to identify targets, trends, and related criminal schemes. They allow law enforcement agencies to coordinate and prioritize investigations, thereby allowing the government to use its limited resources more efficiently. In addition, they provide a partnership between law enforcement and the financial services industry.

In order to foster and develop this partnership, prosecutors and investigators must safeguard these sensitive tools and protect them from disclosure. Financial institutions also value feedback from law enforcement on the utility of the SARs they file. Financial institutions spend a considerable amount of resources on systems to identify and report suspicious activity. They are obligated to do this under the law, but most institutions are eager to support law enforcement's efforts in fighting crime. When they provide substantial assistance, their efforts should be recognized. Prosecutors and agents are encouraged to reach out to the financial community to explain the government's mission, discuss recent law enforcement trends and cases, and encourage the efforts of the financial community in fighting crime and terrorism.❖

ABOUT THE AUTHOR

❑**Lester M. Joseph** is the Principal Deputy Chief in the Asset Forfeiture and Money Laundering Section (AFMLS). He has been a Deputy Chief since the Money Laundering Section was created in 1991. He became Principal Deputy Chief in January 2002. Mr. Joseph joined the Department in 1984 as a Trial Attorney in the Organized Crime and Racketeering Section. From 1981 to 1984, he was an Assistant State's Attorney in Cook County (Chicago), Illinois.✠

Type of Financial Institution	Date of SAR Requirement	31 C.F.R. Cite
Banks	April 1, 1996	103.18
Money Service Business	January 1, 2002	103.20
Broker-Dealers	December 30, 2002	103.19
Casinos	March 25, 2003	103.21
Futures Commission Merchants	May 18, 2004	103.17
Insurance Companies	May 3, 2006	103.16
Mutual Funds	Nov. 1, 2006	103.15

Figure 1

Number of Suspicious Activity Report Filings by Year											
Form	**1996**	**1997**	**1998**	**1999**	**2000**	**2001**	**2002**	**2003**	**2004**	**2005**	**2006**
Depository Institution	62,388	81,197	96,521	120,505	162,720	203,538	273,823	288,343	381,671	522,655	567,080
Money Services Business	-	-	-	-	-	-	5,723	209,512	296,284	383,567	496,400
Casinos and Card Clubs	85	45	557	436	464	1,377	1,827	5,095	5,754	6,072	7,285
Securities & Futures Industries	-	-	-	-	-	-	-	4,267	5,705	6,936	8,129
Subtotal	62,473	81,242	97,078	120,941	163,184	204,915	281,373	507,217	689,414	919,230	1,078,894
Total	**4,205,961**										

Figure 2

Disclosure of Suspicious Activity Reports (SARs)

From: Joshua R. Hochberg
Chief, Fraud Section
Criminal Division
U.S. Department of Justice
July 8, 2003

Suspicious Activity Reports (SARs) provide valuable information that can accelerate the investigation and development of cases for prosecution and provide significant leads for investigations and intelligence. The routine or unnecessary disclosure of SARs or even of their existence undermines the confidentiality surrounding their filing.

Certain financial institutions operating in the United States are required to file reports of known or suspected criminal conduct that takes place at or was perpetrated against the financial institutions. These reports, known as Suspicious Activity Reports or SARs, are filed with the Financial Crimes Enforcement Network (FinCEN), a bureau of the United States Department of the Treasury. SARs are made available to the law enforcement community for use in investigations, prosecutions and related law enforcement activities.

The SAR system was designed to assist the law enforcement community by requiring financial institutions to report transactions that are indicative of possible criminal activity. The required threshold for filing is easily triggered, simply by suspicion, not proof, of criminal activity. The information contained in SARs constitutes raw allegations of the most sensitive kind, precisely because the reported suspicions are unsubstantiated and unproved.

Because financial institutions file SARs with the expectation that they will be accorded sensitive treatment, unnecessary disclosure of SARs could frustrate that expectation and have a chilling effect on both the quantity and the quality of future SAR filings. Moreover, SARs may contain information concerning the methods by which an institution learned of or uncovered suspicious activity, possibly allowing other potential wrongdoers to take action to avoid those methods of detection. Law enforcement agencies and prosecutors should consider SARs similar to confidential source information that, when further investigated, may produce evidence of criminal activity.

Consistent with the treatment accorded confidential source information, the existence of SARs relating to conduct being investigated, as well as the content of SARs, should not normally be disclosed to persons outside the law enforcement community. Disclosure of a SAR should be distinguished from disclosure of the records constituting the transactions discussed in a SAR, such as a wire transfer record, which can be treated as an ordinary piece of evidence. Because the underlying documents prove the transaction, and the SAR does not, it should rarely be necessary to use a SAR in the prosecution's case.

Figure 3

Special Note—Disclosure of SARs and SAR Information to Subjects

Given the nature of the information contained in SARs and the purposes for which such information is collected, there are strict statutory restrictions governing disclosures of SARs, or the fact that SARs have been filed, when these disclosures are made to persons involved in the reported transactions. These provisions recognize that there will be instances in which the disclosure of SARs or their contents is unavoidable due to constitutional or statutory discovery obligations placed on prosecutors.

As amended by the USA PATRIOT ACT (Pub. L. 107-56), 31 U.S.C. 53 18(g) states in relevant part:

> (2) NOTIFICATION PROHIBITED -
>
> (A) IN GENERAL --If a financial institution or any director, officer, employee, or agent of any financial institution, voluntarily or pursuant to this section or any other authority, reports a suspicious transaction to a government agency
>
> (i) the financial institution, director, officer, employee, or agent may not notify any person involved in the transaction that the transaction has been reported; and
>
> (ii) no officer or employee of the Federal Government or of any State, local, tribal, or territorial government within the United States, who has any knowledge that such report was made may disclose to any person involved in the transaction that the transaction has been reported, other than as necessary to fulfill the official duties of such officer or employee.

Under 31 U.S.C. 53l8(g)(2), no government official may disclose a SAR to a person involved in the transaction "other than as necessary to fulfill the official duties of such officer or employee." For example. it may be necessary for a prosecutor to disclose a SAR in situations in which the SAR:

- contains exculpatory or potential impeachment information that a prosecutor is constitutionally obligated to disclose; or
- is a document or contains information required to be disclosed under Fed. R. Crim. P. 16 or the Jencks Act, 18 U.S.C. 3500.

In these and other instances in which a prosecutor believes that disclosure of a SAR to the defense may be compelled by constitutional, statutory or regulatory authority, the prosecutor should consult with supervisory personnel in the office to consider whether the SAR or the material included within the report must be disclosed to the defense, or whether it may be withheld, redacted, limited by protective order or otherwise protected from disclosure.

Attorneys in the Criminal Division's Fraud Section, John Arterberry, Barry Goldman and Jack Patrick (202-514-0890), and Asset Forfeiture and Money Laundering Section, Lester Joseph (202-616-0593), are available for consultation on SAR disclosure issues. Because disclosure of a SAR may affect other investigations or cases and because FinCEN is charged with responsibility for enforcing the SAR laws and regulations, FinCEN's Office of Chief Counsel, 703-905-3590, should be given notice if an office decides to disclose a SAR.

Figure 3 Cont'd

Money Laundering Trends

Emery Kobor
Policy Advisor
Office of Terrorist Financing and Financial Crimes
Department of the Treasury

I. Introduction

Combating money laundering is a massive and evolving challenge which requires a clear and thorough understanding of the various trends and techniques being used by criminals to launder their illicit funds. These trends range from well-established techniques for integrating dirty money into the financial system to modern innovations that exploit global payment networks, as well as the Internet. New and innovative methods for electronic cross-border funds transfer are emerging globally. These new payment tools include extensions of established payment systems, and new payment methods that are substantially different from traditional transactions. New payment methods raise concerns about money laundering and terrorist financing because criminals can adjust quickly to exploit new opportunities that often allow anonymous high value transactions with little or no paper trail or legal accountability. This article is a digest of thirteen different methodologies which were identified in the 2005 Money Laundering Threat Assessment as being used by criminals to launder money in the United States, *available at* http://www.treas.gov/offices/enforcement/pdf/mlta.pdf.

II. Banks and other depository financial institutions

In the United States, only banks and other depository financial institutions are allowed to hold financial deposits and provide direct access to those deposits through the use of paper checks and various bank-to-bank electronic payment networks. Although Money Services Businesses (MSBs) offer an alternative to banks for many financial services, they have to use a depository financial institution to hold their deposits, clear checks, and settle transactions.

Once illicit funds are in a bank, the money can be transferred quickly from account to account, leading to a tangled web of transactions that make it difficult to trace the path or identify the ultimate owner of the money. Criminals open both consumer and business accounts to move illicit cash into the banking system. One technique to avoid a Currency Transaction Report (CTR) being filed is to use "smurfs,"—students, travelers, or other accomplices—to open accounts in a number of banks, then "structure" cash deposits into the accounts by keeping each deposit below the $10,000 CTR threshold. The money launderer will periodically draw down the accounts, transferring funds to other accounts or money laundering vehicles, domestically and offshore.

Bank accounts opened in the name of a business or other legal entity can be useful to disguise the beneficial owner of the account and the true nature of the funds that move through the account. Retail businesses that ring up cash transactions and make nightly deposits can be used as a front to disguise illicit cash added to the day's deposit. Bank accounts held by shell companies and trusts often do not require the disclosure of beneficial ownership and can mask illicit money movement as trade or investment transactions.

III. Correspondent banking

Despite rapid developments in banking technology, domestic bank payment networks around the world generally do not connect with one another. To move money across borders, a U.S. bank often has to hold an account with a bank overseas, a relationship known as correspondent banking. When a U.S. bank customer wants to send a cross-border wire transfer, the bank transfers funds from the correspondent account it holds in the recipient country.

Correspondent accounts and "payable through" accounts create opportunities to use a U.S. or foreign bank without the bank always knowing the true payment originator. A "payable through" account at a U.S. bank involves a foreign bank holding a checking account at the U.S. institution. The foreign bank can issue checks to its customers, allowing them to make payments from the U.S. account. A variation on the "payable through" account is "nesting," in which

foreign banks open correspondent accounts at U.S. banks, but then solicit other foreign banks to use the account. This results in an exponential increase in the number of individuals with access to a single account at a U.S. banking institution.

As cross-border wire transfers come under increased scrutiny and regulation, criminals are using paper checks, money orders, and cashier's checks, as an effective alternative. These more traditional payment instruments take longer to clear when traveling outside the United States, but often receive less scrutiny.

Money launderers can transfer large dollar amounts by writing a number of checks or buying a number of money orders at various U.S. locations, with each payment below the CTR reporting threshold. The dollar-denominated payments are mailed or transported to accomplices overseas who deposit the checks and money orders in foreign bank accounts. Because these are dollar-denominated payments, the foreign banks that receive them have to send them back to the United States for deposit in their U.S. correspondent accounts. Some banks handle as many as five to seven million checks a day. Processing is done as efficiently as possible, making it difficult to aggregate related payments or scrutinize individual payments for evidence of money laundering.

IV. Money services businesses

MSBs provide an alternative to the banking system, offering a full range of financial products and services without the same level of regulation and supervision imposed on banks and other depository financial institutions. Under the Bank Secrecy Act (BSA), 12 U.S.C. §§ 1251-1259, MSBs include the following.

- Currency exchangers.
- Check cashers.
- Issuers of traveler's checks, money orders, or stored value.
- Sellers or redeemers of traveler's checks, money orders, or stored value.
- Money transmitters.

Unlike banks, which are obligated to verify customer identification at account opening, MSBs do not hold customer accounts and are currently obligated, under federal law, to verify and record customer identification only when selling $3,000 or more of money orders or travelers' checks, or conducting a money transfer of $3,000 or more. Most MSBs are required to report suspicious activity, however, excluded from that requirement are check cashers and sellers and redeemers of stored value.

Many MSBs, including the vast majority of money transmitters in the United States, operate through a system of agents. Agents are not required to register with the Financial Crimes Enforcement Network (FinCEN), but are required to establish anti-money laundering (AML) programs and to comply with certain record keeping and reporting requirements.

A. Currency exchangers

Currency exchangers, also referred to as currency dealers, money exchangers, *casas de cambio*, and *bureaux de changes*, exchange bank notes of one country for that of another. Less than ten states currently regulate this activity, which makes it the least regulated MSB category.

Casas de cambio are currency exchange houses specializing in Latin American currencies. In the United States, more than 1,000 *casas de cambio* are located along the border from California to Texas. Some *casas de cambio* exist primarily for money laundering. They take in illicit cash from many clients and then deposit the money under the name of the exchange house. Seized documents in raids conducted by the Venezuelan *Guardia Nacional* in the state of Tachiria revealed that a number of *casas de cambio* were laundering drug proceeds from the United States and routing them through Venezuela to Colombia to avoid the relatively high tariff on U.S. currency in Colombia. Many of the *casas de cambio* involved in the money laundering process have access to U.S. dollar checking accounts through correspondent accounts held by major banks in Venezuela.

B. Check cashers

Money launderers use check-cashing businesses to cash checks that were written to small businesses, but which the launderer purchased with illicit cash. Small businesses benefit by receiving immediate cash, avoiding fees, passing on the risk of bad checks, and potentially evading income taxes. Money launderers sometimes purchase check-cashing businesses outright so that checks can be deposited directly into the launderer's bank account. The lack of record keeping or suspicious

activity report (SAR) filing requirements may hinder law enforcement attempts to trace illicit proceeds through this channel.

C. Money orders

Money orders are attractive to money launderers because they can be issued in large dollar denominations, are less bulky than cash, and are issued anonymously for amounts under $3,000. A common money laundering technique is to structure multiple money order purchases just under the $3,000 customer-identification threshold. It is estimated that more than 830 million money orders, worth more than $100 billion, are issued annually, with 80% issued by the U.S. Postal Service (USPS), Western Union, and MoneyGram International. The remainder are issued by small regional companies.

Money order issuers, other than USPS, rely largely on licensed agents, rather than employees. While the parent firm is responsible for activity across their agent network, it is not required to review individual SARs, and some firms specifically discourage their agents from submitting SARs to the parent firm. Western Union and MoneyGram agents issue more than 50 percent of all money orders in the United States, yet filed only 1 percent of the SARs from October 1, 2002 through December 31, 2004 that involved money orders and money laundering. During the same period USPS, which issues approximately one-quarter of all money orders in the United States, filed 93 percent of the SARs related to money laundering via money orders.

D. Stored value

Stored value, or prepaid cards, operate within either an "open" or "closed" system. Open system cards can be used to make purchases from merchants or to get cash at ATMs that connect to the global payment networks, specifically those operated by Visa and MasterCard. Open system card programs, although issued through banks and other depository institutions, generally do not require a bank account or face-to-face verification of the cardholder's identity. Funds can be prepaid by one person, with someone else in another country accessing the cash via ATM. Open system prepaid cards typically can have additional funds added on an ongoing basis. There are no regulatory guidelines that address customer identification, record keeping, or reporting requirements, regarding open system prepaid card accounts.

Closed system cards can only be used to buy goods or services from the merchant or service provider issuing the card. Examples of closed system cards include store-specific retail gift cards and mass transit system cards. These cards may be limited to the initial value posted to the card or may allow the card holder to add value.

The target markets for prepaid cards include teenagers, people without bank accounts, adults unable to qualify for a credit card, and immigrants sending cash to family outside the United States. Depending on the safeguards employed by the card-issuing bank and its support network, open system prepaid cards may provide an anonymous way to store, transport, and access, illicit cash globally. Closed system cards, primarily store gift cards, present more limited opportunities and a correspondingly lower risk as a means to move monetary value out of the country. Nevertheless, federal law enforcement agencies report both categories of stored value cards are used as alternatives to smuggling physical cash.

E. Money transmitters

The volume and accessibility of money transmitters makes them attractive vehicles to money launderers. Western Union runs the largest nonbank money transmitter network, with more than 245,000 agent locations in 195 countries and territories.

Money transmitters are obligated to verify and record customer identification only when sending a wire of more than $3,000. To evade that threshold, customers can divide up their funds transfers among several wires and several different money transmitters.

Online payment services, including dealers in digital precious metals, are another option for cross-border funds transfers. These intermediaries operate via the Internet and facilitate funds transfers for individuals and businesses by using a variety of payment methods. The forms of payment a service provider accepts and uses to pay out to recipients varies by service provider. Those willing to accept and pay out using anonymous forms of payment (cash, money orders, nonbank wires, and some prepaid cards) create a potential money laundering threat.

U.S. citizens can access payment services online that are based outside of the United States and transfer funds either electronically or by mail. Some online payment services exist to facilitate transactions for online gambling and adult content

that U.S.-based money transmitters typically will not service. Online payment services that offer immediate final settlement with no recourse are often used for illegal transactions and are popular with fraudulent investment schemes.

V. Casinos

As high-volume cash businesses, casinos are susceptible to money laundering, as well as many other financial crimes, and were the first nonbank financial institutions required to develop AML compliance programs. In addition to gaming, casinos offer a variety of financial services including credit, funds transfers, check cashing, and currency exchange.

Tribal casinos are moving rapidly from relative obscurity within the U.S. casino industry to a position of prominence. Collectively, tribal casinos took in $18.5 billion in revenue in 2004—twice the amount generated by Nevada casinos. There are 567 federally recognized American Indian tribes (half are in Alaska), with gaming facilities in twenty-eight states.

Money laundering schemes involving casinos usually start with the purchase of casino chips using illicit cash. The chips then can be used in the following ways.

- Cashed in for a casino check or wire transfer for deposit into a bank account.
- Used as a form of currency for goods and services, particularly illegal narcotics, so that others ultimately cash in the chips.
- Used for gambling in the hope of generating certifiable winnings.

While criminals will structure transactions at banks and MSBs to avoid transaction records or reports that draw attention to them, they use casinos for the opposite purpose. Having a CTR filed on a casino payout has the effect of making the money appear legitimate. Criminals also use casinos to launder counterfeit money, as well as large currency notes that would be conspicuous and difficult to use elsewhere, and which may be marked by undercover law enforcement officers.

VI. Bulk cash smuggling

Increasingly effective AML policies and procedures at U.S. financial institutions may be responsible for money launderers moving illicit cash out of the country to jurisdictions with lax or complicit financial institutions, or to fund criminal enterprises. Smugglers conceal cash in aircraft, boats, vehicles, commercial shipments, express packages, on their person, and in their luggage.

Cash associated with illicit narcotics typically flows out of the United States across the southwest border into Mexico, retracing the route that illegal drugs follow when entering the United States. The cash may stay in Mexico, continue on to a number of other countries, or head back into the United States as a deposit by a bank or *casa de cambio*. Illicit funds leaving the United States also flow into Canada, which also is a source of illegal narcotics.

Cash can be smuggled out of the United States through the 317 official land, sea, and air ports of entry, and any number of unofficial routes along the Canadian and Mexican borders. The United States shares a 3,987 mile border with Canada and a 1,933 mile border with Mexico. In addition to individuals carrying cash over the border, or hiding it in vehicles, it can be hidden in any of the thousands of shipping containers involved in commercial trade with the top two U.S. trading partners (Mexico and Canada).

The extent to which cash smuggled out of the United States is derived from criminal activity other than the sale of illegal drugs is not known. Other cash-intensive sources of illicit income include alien smuggling, bribery, contraband smuggling, extortion, fraud, illegal gambling, kidnapping, prostitution, and tax evasion.

VII. Shell companies and trusts

The United Nations noted, in a 1998 report, that "the principal forms of abuse of secrecy have shifted from individual bank accounts to corporate bank accounts and then to trust and other corporate forms…." OFFICE FOR DRUG CONTROL AND CRIME PREVENTION, UNITED NATIONS, FINANCIAL HAVENS BANKING SECRECY AND MONEY LAUNDERING 57 (1998). Legal entities, such as shell companies and trusts, can use bearer shares and nominee shareholders and directors to hide ownership and mask financial transactions.

Legal jurisdictions, whether states within the United States or entities elsewhere, that offer strict secrecy laws, lax regulatory and supervisory regimes, and corporate registries that safeguard anonymity, are obvious targets for money launderers. A handful of U.S. states offer

company registrations with secrecy features—such as minimal information requirements and limited oversight—that rival those offered by offshore financial centers. Delaware, Nevada, and Wyoming, are often cited as the most accommodating jurisdictions in the United States for the organization of these legal entities.

Intermediaries, called nominee incorporation services, establish U.S. shell companies and bank accounts on behalf of foreign clients. By hiring a firm to serve as an intermediary, the true owners of a shell company, or other legal entity, may avoid disclosing their identities in state corporate filings and in the documentation used to open corporate bank accounts.

Several options are available in the formation of legal entities that allow beneficial owners even greater anonymity. Bearer shares are negotiable instruments that accord ownership of a company to the person who possesses the share certificate. Bearer share certificates do not contain the name of the shareholder and are not registered, with the possible exception of their serial numbers. Accordingly, these shares provide for a high level of anonymity and are easily negotiable.

Nominee shareholders can be used in privately-held companies as stand-ins to shield beneficial ownership information. Where nominee shareholders are allowed, the usefulness of the shareholder register is undermined because the shareholder of record may not be the ultimate beneficial owner. Similarly, nominee directors and companies serving as directors of a legal entity may conceal who really controls the company.

Trusts separate legal ownership from beneficial ownership and are useful when assets are given to minors or individuals who are incapacitated. The trust creator transfers legal ownership of the assets to a trustee, which can be an individual or a corporation. The trustee manages the assets on behalf of the beneficiary, based on the terms of the trust deed. Although trusts have many legitimate applications, they can also be misused. Trusts enjoy a greater degree of privacy and autonomy than other corporate vehicles, as virtually all jurisdictions recognizing trusts do not require registration or central registries and there are few authorities charged with overseeing trusts. In most jurisdictions, no disclosure of the identity of the beneficiary or the creator of the trust is made to authorities.

VIII. Trade-based money laundering

Money launderers use fraudulent foreign trade transactions as a way to provide cover for, and legitimize, funds transfers using illicit proceeds. Trade-based money laundering encompasses a variety of schemes that involve over- and under-invoicing, double invoicing, and misclassification of the goods shipped.

The most common method of trade-based money laundering in the Western Hemisphere is the Black Market Peso Exchange (BMPE), which is responsible for moving an estimated $5 billion worth of drug proceeds per year from the United States to Colombia. The scheme allows drug traffickers to exchange their illicit dollars in the United States for clean pesos in Colombia, without physically moving funds from one country to the other. *See* David Marshall Nissman, *The Columbia Black Market Peso Exchange*, UNITED STATES ATTORNEYS' BULLETIN, June 1999, at 31.

Money brokers act as intermediaries between the drug traffickers in the United States who hold dollars, but want pesos, and Colombian businessmen who hold pesos, but want dollars to purchase goods for import. The money brokers buy the illicit dollars in the United States and enlist smurfs to buy money orders or deposit the cash in U.S. bank accounts. The money is then used to purchase U.S. products which are exported to Colombia and elsewhere. The Colombian importers complete the money laundering cycle by paying the money broker for the U.S. merchandise with pesos, which are transferred to the drug dealers.

Access to U.S. dollars is regulated by the Colombian government. Before pesos can be exchanged for dollars, the importer has to demonstrate that government import permits have been obtained, thereby insuring that the applicable Colombian duties and taxes will be collected. Colombian businesses bypass the government levies by dealing with BMPE brokers. See Figure 1, page 20.

A similar scheme to evade Colombian taxes involves *reintegro*, which means "reintegrate papers." When goods are exported from Colombia, the shipper must obtain official documents that clear the goods for export and allow payment to be received into the shipper's bank account. After the initial use of the export documents, these papers are often sold for others

to use, creating an opportunity to repatriate drug proceeds disguised as payments for exports.

In addition to the import and export of conventional goods, precious gems and metals can be used as an alternative to cash to transfer value across borders. Like gold and other precious metals, diamonds are attractive to money launderers because they are easily concealed and transported, and because they are mined in remote areas of the world and are virtually untraceable to their original source. Even when diamonds are transported openly, it is relatively easy to mislabel their value for money laundering purposes.

IX. Life insurance and investments

Life, health, and accident insurance, generate more than half a trillion dollars in premiums and contract revenue annually for U.S. insurers. Much of this revenue stream actually comes from the sale of annuities, contracts that guarantee a fixed or variable payment over a given period of time. While whole and term life insurance policies remain an important part of the business, insurance agents and brokers are now often investment advisers selling a variety of financial products. The expansion from insurance policies to investment products has substantially increased the money laundering threat posed by the insurance industry.

Life insurance policies that can be cashed in are an inviting money laundering vehicle because criminals are able to put "dirty" money in and take "clean" money out in the form of an insurance company check. An alternative money laundering vehicle is to purchase life insurance with illegal proceeds and then borrow against the policy. Similarly, annuity contracts allow a money launderer to exchange illicit funds for an immediate or deferred "clean" income stream. These vulnerabilities generally do not exist in products offered by property and casualty insurers, or by title or health insurers.

Money launderers exploit the fact that insurance products are often sold by independent brokers and agents who do not work directly for the insurance companies. These intermediaries may have little know-how or incentive to screen clients or question payment methods. In some cases, agents take advantage of their intermediary status to collude with criminals against insurers to perpetrate fraud or facilitate money laundering.

X. Conclusion

The United States has a robust and aggressive AML program. As it becomes more difficult to move illicit funds using a particular money laundering method, there is a clear migration to other channels. The Financial Action Task Force recognized the effectiveness of the United States. AML enforcement regime in its Report on the Third Mutual Evaluation of the United States, adopted in June 2006, *available at* http://www.fatf-gafi.org/dataoecd/44/12/37101706.pdf. The Report's summary states: "The U.S. Authorities are committed to identifying, disrupting, and dismantling money laundering and terrorist financing networks. They seek to combat money laundering and terrorist financing on all fronts, including by aggressively pursuing financial investigations. These efforts have produced impressive results in terms of prosecutions, convictions, seizures, asset freezing, confiscation and regulatory enforcement actions."❖

ABOUT THE AUTHOR

❑**Emery Kobor** advises Treasury policymakers on a range of issues, but focuses primarily on identifying emerging money laundering and terrorist financing threats associated with global payment and communications networks. Emery chaired the intergovernmental working group that produced the 2007 National Money Laundering Strategy and was the principal author of the first U.S. Money Laundering Threat Assessment, published in 2005. He served as co-chair of the international Financial Action Task Force working group that produced the Report on New Payment Methods, published in October 2006. Prior to joining the Department of the Treasury in 2004, Emery worked as a consultant, advising corporate treasurers on payment and risk management strategies and was a senior research analyst for the Federal Reserve Bank of Chicago's Payments Studies Group.✠

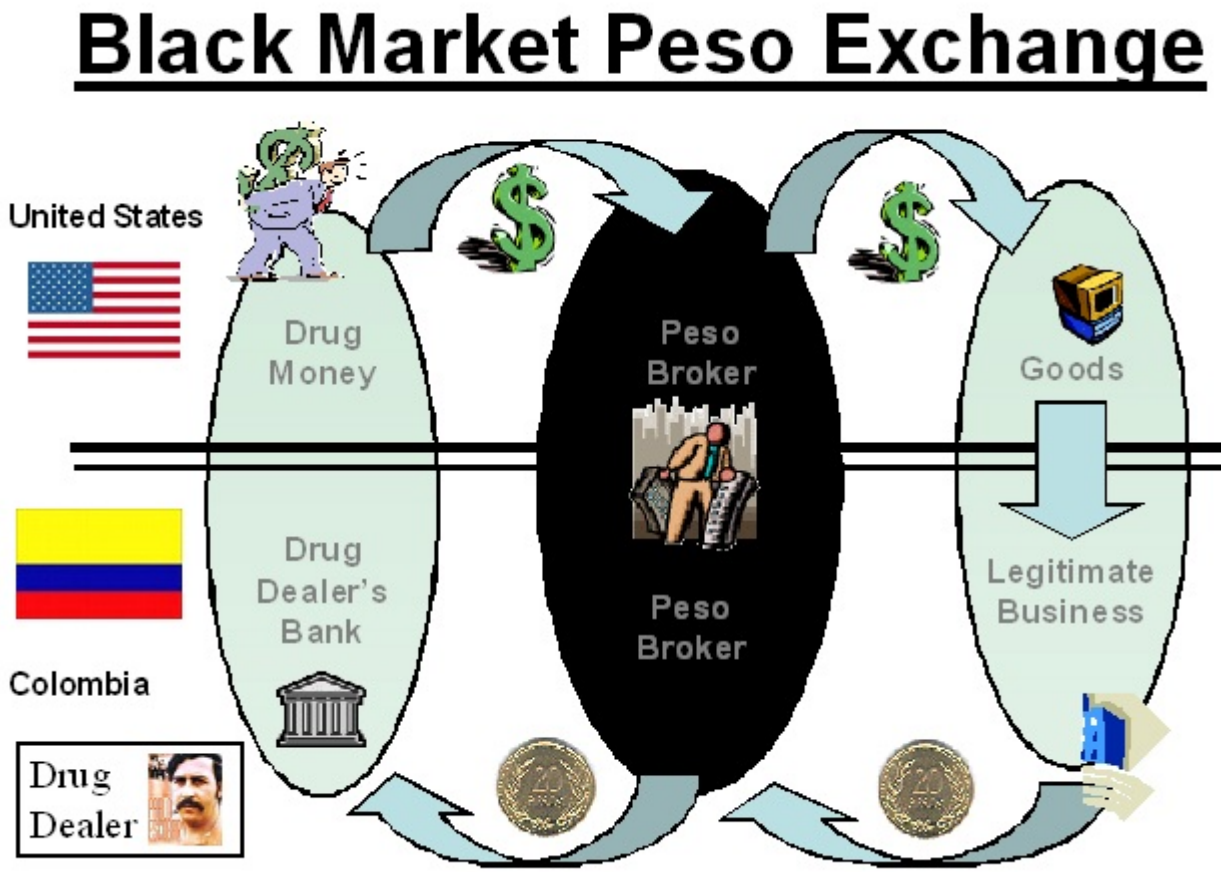
Black Market Peso Exchange
United States
Drug Money
Peso Broker
Goods
Drug Dealer's Bank
Peso Broker
Legitimate Business
Colombia
Drug Dealer

Figure 1

The Money Laundering Statutes (18 U.S.C. §§ 1956 and 1957)

Stefan D. Cassella
Deputy Chief for Legal Policy
Asset Forfeiture and Money Laundering Section
Criminal Division

I. Introduction

The principal money laundering statutes are 18 U.S.C. §§ 1956 and 1957. Section 1956 consists of three provisions dealing with domestic money laundering, international money laundering, and undercover "sting" cases, respectively. *See* 18 U.S.C. § 1956(a)(1), (a)(2), and (a)(3). Section 1957 makes it an offense simply to conduct any monetary transaction in criminal proceeds involving more than $10,000. This article will focus first on the elements of the domestic money laundering statute, § 1956(a)(1), and then will point out the similarities and differences between this statute and the other three.

II. Section 1956(a)(1)

A domestic money laundering offense under Section 1956(a)(1) is committed if the defendant:

- Knowing that certain property represents the proceeds of some form of unlawful activity; and
- Intending to
  - a. promote the carrying on of the specified unlawful activity, or
  - b. engage in conduct that violates 26 U.S.C. §§7201 or 7206, or
  - c. conceal or disguise the nature, location, source, ownership, or control of the proceeds of the specified unlawful activity, or
  - d. avoid a transaction reporting requirement;
- Uses the property, which is in fact the proceeds of a specified unlawful activity (SUA);
- To conduct or attempt to conduct a financial transaction affecting interstate commerce.

The *actus reus* of the crime is the financial transaction. The remaining elements are mental states (knowledge and intent) or factual predicates (the property must be SUA proceeds; the transaction must affect interstate commerce) that must be present at the time of the financial transaction. Thus, in any money laundering case, it is best for the prosecutor to focus first on which financial transaction will serve as the basis for the money laundering. See Figure 1, page 32.

A. Financial transaction

The terms "transaction" and "financial transaction" are defined in § 1956(c)(3) and (4). In short, virtually anything that can be done with money is a financial transaction—whether it involves a financial institution, another kind of business, or even private individuals. Thus, the simple transfer of cash from one person to another may constitute a money laundering offense. *See United States v. Otis*, 127 F.3d 829 (9th Cir. 1997) (drug dealer's delivery of cash to a money launderer is a financial transaction). Other examples abound in the case law. *See United States v. Herron*, 97 F.3d 234, 237 (8th Cir. 1996) (wire transfer through Western Union is a financial transaction); *United States v. Rounsavall*, 115 F.3d 561 (8th Cir. 1997) (writing check to purchase cashier's checks is financial transaction); *United States v. Brown*, 31 F.3d 484, 489 n.4 (7th Cir. 1994) (processing credit card charges involves "payment, transfer, or delivery by, through, or to a financial institution").

Note that the transaction does not need to involve money or other monetary instruments. Simply transferring title to certain kinds of property, such as land or vehicles, falls within the statutory definition of a financial transaction. *See United States v. Hall*, 434 F.3d 42, 52 (1st Cir. 2006) (recording a mortgage is a financial transaction); *United States v. Carrell*, 252 F.3d 1193, 1207 n.14 (11th Cir. 2001) (transfer of title to real property is a financial transaction under section 1956(c)(4)); *United States v. Westbrook*, 119 F.3d 1176 (5th Cir. 1997) (purchase of a vehicle is a financial transaction because it

involves transfer of title); 18 U.S.C. § 1956(c)(4)(A)(iii).

The only serious limitation, in the case law, is that the simple transportation of cash from point A to point B by a single individual may not be a financial transaction. There has to be a transfer or disposition of the cash between two people. *See United States v. Puig-Infante*, 19 F.3d 929 (5th Cir. 1994) (transporting drug proceeds from Florida to Texas was *not* a "transaction," absent evidence of disposition once cash arrived at a destination). *But see United States v. Elso*, 422 F.3d 1305, 1310 n.7 (11th Cir. 2005) (defendant who retrieves third party's money from third party's house, puts it in his car, and drives away, conducts a "transaction").

This limitation aside, finding a financial transaction that will satisfy the statutory definition is generally not difficult for the prosecutor. Indeed, the typical crime, conducted for profit, will involve a whole series of financial transactions. The issue for the prosecutor, therefore, is choosing which financial transaction to use as the basis for the criminal charge.

This choice is critical for many reasons. First, most courts hold that each financial transaction is a separate offense. Because the unit of prosecution is the financial transaction, and because charging multiple transactions as a continuing course of conduct in a single count is duplicitous, the prosecutor is forced to choose one financial transaction for each count in the indictment. *See United States v. Prescott*, 42 F.3d 1165, 1166 (8th Cir. 1994) (charging multiple financial transactions as a continuing course of conduct in a single count is duplicitous); *United States v. Huber*, 2002 WL 257851, *1 (D.N.D. Jan. 3, 2002) (Congress intended each financial transaction to constitute a separate offense, "[t]hus, there is no doubt that the Government must charge a specific financial transaction for each substantive money laundering count," citing legislative history). *But see United States v. Moloney*, 287 F.3d 236, 241 (2d Cir. 2002) ("a single money laundering count can encompass multiple acts provided that each act is part of a unified scheme"); *United States v. Gordon*, 990 F. Supp. 171 (E.D.N.Y. 1998) (single money laundering count charging multiple financial transactions *not* duplicitous where all transactions were part of single continuous scheme).

Moreover, the choice of the financial transaction fixes the time at which the other elements apply. That is, the defendant must have the requisite knowledge and intent, and the property must represent SUA proceeds, *at the time the financial transaction takes place*. *See United States v. Hughes*, 230 F.3d 815, 820-21 (5th Cir. 2000) (defendant must know money was criminal proceeds at the time he conducts the money laundering transaction); *United States v. Puig-Infante*, 19 F.3d 929, 938-39 (5th Cir. 1994) (drug deal is not a money laundering offense because money exchanged for drugs is not proceeds at the time the financial transaction takes place).

The financial transaction also determines venue, *see United States v. Cabrales*, 524 U.S. 1 (1998) (venue for money laundering lies where the financial transaction occurred), and it determines the timing of the money laundering offense for statute of limitations purposes. *See United States v. Blackwell*, 954 F. Supp. 944, 956 (D.N.J. 1997) (statute of limitations begins to run when the financial transaction is initiated), following *United States v. Li*, 55 F.3d 325, 330 (7th Cir. 1995). Finally, the choice of the financial transaction determines what property is going to be subject to forfeiture. *See* 18 U.S.C. §§ 981 and 982 (only property "involved in" the financial transaction is subject to forfeiture).

B. Interstate commerce

After some debate, the courts have concluded that the effect on interstate commerce is an element of the offense that the government must allege in the indictment and prove beyond a reasonable doubt. *See United States v. Evans*, 272 F.3d 1069, 1081 (8th Cir. 2001) ("[a]n effect on interstate commerce is an essential element of money laundering."); *United States v. Ladum*, 141 F.3d 1328 (9th Cir. 1998) (interstate commerce is both jurisdictional and an essential element of the offense); *United States v. Allen*, 129 F.3d 1159 (10th Cir. 1997) (in a section 1957 case, the interstate commerce requirement is both jurisdictional and an essential element of the offense and must be decided by a jury).

Showing a small impact is, however, sufficient. Very frequently, the government will simply show that the transaction involved an Federal Deposit Insurance Corporation (FDIC)-insured bank or was commercial in nature. *See United States v. Peay*, 972 F.2d 71 (4th Cir. 1992) (transaction involving funds on deposit at a financial institution insured by FDIC affects interstate commerce); *United States v. Kunzman*,

54 F.3d 1522 (10th Cir. 1995) (same); *United States v. Trammell*, 133 F.3d 1343 (10th Cir. 1998) (depositing checks drawn on FDIC-insured bank and wiring money from bank in one state to bank in another affects interstate commerce); *United States v. Jackson*, 935 F.2d 832 (7th Cir. 1991) (transaction involving check drawn on a bank implicates interstate commerce); *United States v. Ripinsky*, 109 F.3d 1436, *opinion amended on denial of reh'g*, 129 F.3d 518 (9th Cir. 1997) (if the transaction is commercial in nature, government need only prove that it had a minimal effect on interstate commerce that, through repetition by others, could have a substantial effect).

C. Knowledge

The government must show that, *at the time the financial transaction occurred*, the money launderer knew that the property in the financial transaction was dirty money. Specifically, he must know that the property represented the proceeds of "some form" of unlawful activity, but he does not need to know precisely what the unlawful activity was. *See* 18 U.S.C. § 1956(c)(1). In other words, it is not a defense for the defendant to say, "I did not know it was drug money, I thought it was the proceeds of insurance fraud." *See United States v. Turner*, 400 F.3d 491, 496 (7th Cir. 2005) (defendant need not know actual source of the money, but only that it came from some "illegal activity"); *United States v. Rivera-Rodriguez*, 318 F.3d 268, 271 (1st Cir. 2003) ("defendant is not required to know what type of felony spawned the proceeds but only that some felony did so."); *United States v. Reiss*, 186 F.3d 149, 154 (2d Cir. 1999) (defendant need only know money is criminally derived; he does not need to know it is drug proceeds); *United States v. Marzano*, 160 F.3d 399, 400 (7th Cir. 1998) (if defendant thought he was laundering drug money, the fact that he actually laundered embezzlement proceeds would not be a defense).

The question most prosecutors face is how to prove a defendant knew the money he was laundering for someone else was illegally derived? As with other issues involving a mental state, the proof is usually circumstantial and the case law provides many examples.

For instance, in *United States v. Golb*, 69 F.3d 1417 (9th Cir. 1995), the court held that the jury could infer that the defendant, who brokered an airplane sale, (1) knew that the purchase money was illegally derived because the money came as multiple, anonymous wire transfers and bundles of checks, (2) made statements about the purchaser's involvement in drug trafficking, and (3) made threats of violence, showing he knew he was not representing a legitimate business person. *See United States v. Otis*, 127 F.3d 829, 835 (9th Cir. 1997) (defendant's "pager contacts, associations, and criminal history" sufficient to show that defendant knew the $60,000 he turned over to third-party in parking lot was criminal proceeds); *United States v. Hurley*, 63 F.3d 1 (1st Cir. 1995) (even underlings who never dealt with drug dealers knew that money they were laundering was drug proceeds because no other cash-generating business would require the laundering of such huge quantities of cash); *United States v. Campbell*, 977 F.2d 854 (4th Cir. 1992) (real estate agent willfully blind to client's use of drug proceeds to purchase house).

Similarly, in *United States v. Bornfield*, 145 F.3d 1123 (10th Cir. 1998), the Tenth Circuit held that an accountant had actual knowledge that his client's cash came from drug dealing because the accountant (1) prepared the drug dealer's tax returns, (2) knew he sold drugs, and (3) knew he had insufficient legitimate income.

D. Proceeds

The third element of money laundering under Section 1956(a)(1) is that the property in the financial transaction was, *in fact,* the proceeds of an offense constituting "specified unlawful activity." The offenses listed in § 1956(c)(7), and all of the RICO predicates listed in 18 U.S.C. § 1961(1), qualify as SUAs. In addition, certain violations of foreign law, including offenses against a foreign country involving drug trafficking, kidnapping, robbery, extortion, bank fraud, murder, and destruction of property by means of explosives or fire, are SUAs. *See* § 1956(c)(7)(B).

Proving the property is SUA proceeds is easy, if the prosecutor can trace the money to a particular offense. It is not, however, necessary to do this. The courts unanimously hold that showing the SUA generated the money or other property, without identifying the date and place of the offense, is sufficient. For example, in *United States v. Golb*, 69 F.3d 1417 (9th Cir. 1995), evidence that the money came from an account used by professional money launderers to launder drug proceeds was sufficient to establish the "proceeds" element. Similarly, in *United States v. Blackman*, 904 F.2d 1250, 1257

(8th Cir. 1990), the government proved that the property in the financial transaction was drug proceeds by showing that the defendant was engaged in the drug business and was using wire services to move a lot of cash. The government also called an expert witness to testify that these transactions were typical of what drug dealers do with drug money. *See also United States v. Hardwell*, 80 F.3d 1471 (10th Cir. 1996) (evidence that the defendant was engaged in drug trafficking and had insufficient legitimate income to produce the money used in the financial transaction was sufficient); *United States v. Herron*, 97 F.3d 234, 237 (8th Cir. 1996) (same); *United States v. Eastman*, 149 F.3d 802 (8th Cir. 1998) (following *Blackman*; no need to trace proceeds to particular drug sale; government may rely on defendant's involvement in drug trade and lack of legitimate income to prove wired money was drug proceeds).

As these cases illustrate, prosecutors commonly prove that the property is SUA proceeds with circumstantial evidence. *See United States v. Gotti*, 459 F.3d 296, 337 (2d Cir. 2006) (multitude of illegal activities of organized crime family provided sufficient circumstantial evidence that the money they laundered was SUA proceeds); *United States v. Pizano*, 421 F.3d 707, 723 (8th Cir. 2005) (defendant's lack of legitimate income, cash deposits into her account, and conduct of transactions on behalf of brother who is a drug dealer, sufficient to establish that funds defendant used to purchase real property were brother's drug proceeds); *United States v. Misher*, 99 F.3d 664 (5th Cir. 1996) (when defendant, who is connected to drug trafficking, pays for a car with suitcase full of cash, there is sufficient evidence that the money is SUA proceeds).

Note that only part of the money involved in the financial transaction needs to be SUA proceeds; proving "that the funds in question came from an account in which tainted proceeds were commingled with other funds is sufficient." *United States v. Garcia*, 37 F.3d 1359, 1365 (9th Cir. 1994). *See United States v. Huber*, 404 F.3d 1047, 1058 (8th Cir. 2005) (the presence of legitimate funds does not make a money laundering transaction lawful; it is only necessary to show that the transaction *involves* criminal proceeds); *United States v. Bieganowski*, 313 F.3d 264, 279-80 (5th Cir. 2002) (even if some of health care provider's income was legitimate, transfer of commingled funds would satisfy the proceeds element of § 1956(a)(1)); *United States v. Rodriguez*, 278 F.3d 486, 491 (5th Cir. 2002) (jury was free to convict alien smuggler of money laundering despite evidence that he used commingled funds to conduct his financial transactions).

E. Merger issue

The most troublesome issue involving the proceeds element is the requirement that the property be SUA proceeds *at the time the financial transaction takes place*. If the financial transaction constituting the underlying crime and the money laundering offense take place simultaneously, the two offenses are said to "merge." In this instance, the money laundering prosecution fails because no separate money laundering offense occurred.

For example, if a drug sale takes place on a street corner, there is clearly a financial transaction, but the transaction does not involve SUA proceeds at the time it takes place because the seller does not receive proceeds until the sale is complete. For there to be a money laundering offense, a subsequent, "downstream" transaction, such as the deposit of the sale proceeds into a bank account, must occur. *See United States v. Butler*, 211 F.3d 826, 830 (4th Cir. 2000) ("the laundering of funds cannot occur in the same transaction through which those funds first become tainted by crime"); *United States v. Richard*, 234 F.3d 763, 769 (1st Cir. 2000) (same; quoting *Butler*); *United States v. Mankarious*, 151 F.3d 694, 706 (7th Cir. 1998) (the acts that produce the proceeds being laundered must be distinct from the conduct that constitutes money laundering); *United States v. Carucci*, 364 F.3d 339, 345-46 (1st Cir. 2004) (conviction reversed because evidence did not establish that the SUA offense occurred before the money laundering transaction); *United States v. Howard*, 271 F. Supp. 2d 79, 84-90 (D.D.C. 2002) (the money laundering statutes criminalize transactions in proceeds, not the transactions that create the proceeds; extended discussion of merger cases).

The merger of the money laundering transaction and the underlying SUA is a big problem in fraud cases where it is often unclear whether the transaction is simply part of the fraud, or is a downstream transaction constituting a separate money laundering offense. As a general principle, prosecutors should only charge money laundering where the fraud scheme has matured to the point where it has yielded proceeds that fall, directly or indirectly, within the defendant's

control, and the defendant then conducts a separate downstream transaction. *See United States v. Johnson*, 971 F.2d 562 (10th Cir. 1992) (where a defendant fraudulently induces a victim to wire transfer funds directly to the defendant's account, such transfer *does not* constitute money laundering, because funds were not "criminally derived" at the time the transfer took place; if, however, the transaction involved two steps—with defendant first obtaining money from victim and then making deposit—the second step would be a § 1957 violation); *United States v. Savage*, 67 F.3d 1435 (9th Cir. 1995) (wire transfer out of bank account constitutes § 1957 violation where defendant had control over the account at the time the transfer was made, even though it was not in his name; distinguishing *Johnson* where defendant did not have control over victim's money until the transfer was complete); *United States v. Estacio*, 64 F.3d 477 (9th Cir. 1995) (no violation of merger rule where proceeds of earlier phase of check kiting scheme were used to continue the scheme). *But see United States v. Christo*, 129 F.3d 578 (11th Cir. 1997) (distinguishing *Estacio*; if transaction is the first and only step in a check kiting scheme, it does not involve SUA proceeds because no bank has yet lost any money).

It is not necessary that the fraud scheme be complete. The money laundering offense may constitute one step in the scheme, but the scheme must have reached a point where it has yielded proceeds before the defendant can be guilty of committing a money laundering offense. *See United States v. Thomas*, 451 F.3d 543, 548-49 (8th Cir. 2006) (checks that defendant obtained from victims were "proceeds obtained from ongoing fraudulent activities" when he cashed them or deposited them into a bank account; it is not necessary for the underlying fraud to be complete; distinguishing *Johnson* and following *Mankarious*); *United States v. Richard*, 234 F.3d 763, 770 (1st Cir. 2000) (checks that defendant received from investors and intended to conceal from bankruptcy court were proceeds of completed phase of bankruptcy scheme, and subsequent transactions were money laundering offenses even though the bankruptcy fraud was not yet complete; following *Mankarious*); *United States v. Castellini*, 392 F.3d 35, 49 (1st Cir. 2004) (SUA need not be complete for it to yield proceeds; money becomes proceeds of § 152 bankruptcy fraud as soon as debtor gives it to third party to hide for him, even though no bankruptcy petition has yet been filed; what third party does with the money is a money laundering offense).

F. Inconsistent verdicts; acquittal on the SUA

There have been a number of cases where the defendant was acquitted on the underlying SUA offense but convicted of money laundering. Of course, nothing is wrong with this if the defendant is convicted of laundering the proceeds of an offense committed by someone else. Nevertheless, if the government charges the defendant with laundering the proceeds of his own illegal conduct, whether such inconsistent verdicts will be upheld depends on how the indictment is drafted.

If the indictment charges the defendant with laundering the proceeds of a particular crime but does not refer to specific counts in the indictment, the defendant may be convicted of money laundering, even though he is acquitted on the counts charging the underlying crime. In this instance, the jury could have found that the property being laundered was the proceeds of crimes other than those alleged in the indictment, or that the crimes alleged in the indictment were committed by someone other than the defendant. *See United States v. Magluta*, 418 F.3d 1166, 1174 (11th Cir. 2005) (defendant's acquittal in separate drug prosecution does not estop government from using same drug offenses to prove the proceeds element of money laundering; jurors may have acquitted defendant because they believed someone else committed the drug offenses); *United States v. Whatley*, 133 F.3d 601 (8th Cir. 1998) (money laundering conviction affirmed notwithstanding jury's acquittal on underlying fraud SUA, as long as there was sufficient evidence to support finding that laundered funds were SUA proceeds).

Where, however, the money laundering count alleges that the defendant laundered the proceeds of specific counts in the indictment, and the conviction on those counts is reversed, the money laundering conviction must be vacated as well. *United States v. Adkinson*, 135 F.3d 1363 (11th Cir. 1998). Therefore, prosecutors should be careful to draft money laundering counts charging the defendant with laundering the proceeds of an offense or scheme generally, *e.g.*, the property was the proceeds of SUA, to wit: a scheme to defraud in violation of 18 U.S.C. § 1343—and *not* the proceeds of specific counts.

G. Specific intent

At the time of the financial transaction, the defendant must act with one of four specific intents. These are alternative mental intents that the government may allege in the conjunctive in the indictment and in the disjunctive in the jury instructions. *See United States v. Navarro*, 145 F.3d 580 (3d Cir. 1998) (alternative intents should be charged in the conjunctive and the jury instructed in the disjunctive; no unanimity instruction required); *United States v. Holmes*, 44 F.3d 1150 (2d Cir. 1995) (it is multiplicitous to charge defendant in multiple counts with violations of different subsections of § 1956(a)(1) based on same financial transaction).

Intent to promote. The defendant violates the money laundering statute if he conducts a financial transaction with the intent to promote any SUA. *See* 18 U.S.C. § 1956(a)(1)(A)(i). This is called "promotion money laundering."

Commonly, prosecutors prove promotion money laundering by showing that the defendant reinvested the proceeds of his offense to keep the scheme going. The case law is filled with examples of this so-called "plowing back" of the proceeds. *See United States v. Lawrence*, 405 F.3d 888, 901 (10th Cir. 2005) (using proceeds of Medicare fraud scheme to pay doctor whose participation was essential to the scheme and keep "the doors of the clinic open" promoted the scheme and was not use of ordinary business expenses); *United States v. Grasso*, 381 F.3d 160, 168-69 (3d Cir. 2004) (reinvesting proceeds of fraudulent scheme to cover advertising, printing, and mailing expenses, was promotion money laundering), *cert. granted and judgment vac'd*, 544 U.S. 945 (2005) (remanded for consideration in light of *Booker* decision); *United States v. Marbella*, 73 F.3d 1508 (9th Cir. 1996) (using fraud proceeds to pay commissions to persons who brought in more victims promoted SUA).

Courts have also found the "promotion" element satisfied where the defendant used SUA proceeds to lull new victims into his scheme or to avoid detection. *See United States v. Ismoila*, 100 F.3d 380 (5th Cir. 1996) (defendant promoted scheme to defraud credit card issuers by depositing credit card receipts into business bank account because it gave appearance that defendant was operating a legitimate business that accepted credit card payments for merchandise); *United States v. Hand*, 76 F.3d 393 (10th Cir. 1995) (unpublished) (using proceeds to create "aura of legitimacy" for benefit of victims promotes fraud scheme); *United States v. Savage*, 67 F.3d 1435 (9th Cir. 1995) (transferring money to Europe lent "aura of legitimacy" to defendant's fraudulent claim that he was investing victim's money in European investment business). Of course, it is also an offense to use the proceeds of one crime to commit an entirely separate crime.

Intent to evade income taxes. The second intent alternative is to prove that the defendant laundered the SUA proceeds with the intent to evade income taxes. *See* 18 U.S.C. § 1956(a)(1)(A)(ii); *United States v. Suba*, 132 F.3d 662 (11th Cir. 1998) (defendant's failure to report three checks on his income tax return is evidence that he laundered them with intent to evade taxes). In these cases, Tax Division authorization is required for any prosecution under § 1956(a)(1)(A)(ii) where the purpose of the financial transaction was to evade paying taxes.

Intent to conceal or disguise. The most commonly alleged money laundering offense is the one that involves a financial transaction conducted with the intent to conceal or disguise the nature, source, location, ownership, or control, of the SUA proceeds. *See* 18 U.S.C. § 1956(a)(1)(B)(i). This is called "concealment money laundering." Almost always, the prosecutor will have to prove intent to conceal or disguise by circumstantial evidence.

One way this is done is to show that the defendant engaged in unusual or convoluted transactions that would make no sense unless his purpose was to conceal or disguise. For example, in *United States v. Tencer*, 107 F.3d 1120 (5th Cir. 1997), the Fifth Circuit held that depositing proceeds into geographically distant bank accounts, sending the proceeds (commingled with untainted funds) to a mail drop address, and trying to convert all of the proceeds to cash as investigators closed in, all indicated an intent to conceal, although the defendant conducted the transactions in his own name. *See also United States v. Morales-Rodriguez*, 467 F.3d 1, 13 (1st Cir. 2006) (monthly secretive transfers of funds between three separate bank accounts was an attempt to conceal the nature, location, source, ownership, and control, of proceeds); *United States v. Magluta,* 418 F.3d 1166, 1177 (11th Cir. 2005) (moving cash from Miami to New York to Israel, where it was deposited in an account in a false name, was sufficient to show

that when defendant paid his lawyer with check drawn on that account, he intended to conceal the source of the money); *United States v. Turner*, 400 F.3d 491, 496-98 (7th Cir. 2005) (use of interest-free loans, putting property in name of third party, structuring deposits, and traveling to out-of-town banks to conduct transactions involving cashier's checks all show intent to conceal or disguise).

Intent to conceal or disguise can also be shown by evidence that the defendant conducted the transaction in the name of a third-party or legitimate business. *See United States v. Hall*, 434 F.3d 42, 53 (1st Cir. 2006) (having sister purchase a money order in her name was evidence of intent to conceal the source of money used to purchase a vehicle); *United States v. Cruzado-Laureano,* 404 F.3d 470, 483 (1st Cir. 2005) (corrupt mayor who deposited extortion checks payable to wife's dental practice into her account had intent to conceal; that he was well-known in the bank is no defense); *United States v. Shepard*, 396 F.3d 1116, 1122-23 (10th Cir. 2005) (depositing fraud proceeds in bank account of family member shows intent to conceal); *United States v. Ladum*, 141 F.3d 1328 (9th Cir. 1998) (having tenants pay rent checks to nominee conceals true ownership of property on which rent is paid); *United States v. Suba*, 132 F.3d 662 (11th Cir. 1998) (defendant invested fraud proceeds in securities and real estate through children's trust fund after forging trustee's name).

Likewise, intent to conceal or disguise can be shown by evidence that the defendant intentionally commingled the SUA proceeds with other funds. *See United States v. Griffith*, 85 F.3d 284 (7th Cir. 1996) (commingling funds from legitimate and illegal businesses and funneling proceeds of illegal activities through legitimate financial channels shows intent to conceal); *United States v. Posters N Things Ltd.*, 969 F.2d 652, 661 (8th Cir. 1992), *aff'd on other grounds*, 114 S. Ct. 1747 (1994) (commingling dirty money with revenue from legitimate business in common account); *United States v. Rutgard*, 108 F.3d 1041 (9th Cir. 1997) (dicta) (commingling criminally derived cash with innocently derived funds can show intent to conceal or disguise identity of tainted money).

In some cases, courts have held that simply converting SUA proceeds into goods and services violated the "conceal or disguise" prong of the statute. For example, in *United States v. Norman*, 143 F.3d 375 (8th Cir. 1998), the Eighth Circuit held that the purchase of a car constituted a violation of § 1956(a)(1)(B)(i), because it concealed what happened to the SUA proceeds. In other words, converting the money from one form to another, e.g., bank deposits into consumer goods, may constitute a money laundering offense, if the transaction is designed to conceal or disguise the SUA proceeds. *See United States v. Martinez-Medina*, 279 F.3d 105, 115-16 (1st Cir. 2002) (purchasing consumer items through third parties with cash from drug sales supports inference of intent to conceal); *United States v. Heater*, 63 F.3d 311 (4th Cir. 1995) (use of large quantities of cash to buy vehicles and real property, using third-party names and addresses, showed intent to conceal or disguise drug proceeds by purchasing merchandise); *United States v. Wynn*, 61 F.3d 921 (D.C. Cir. 1995) (drug dealer who spent hundreds of thousands of dollars on expensive clothes with cooperation of merchant who recorded sales in false names intended to conceal or disguise drug money by converting it to goods).

In other cases, however, where the defendant simply spent the SUA proceeds and made no effort to conceal or disguise either his identity or the source of the funds, the evidence was insufficient to establish a violation of this prong of § 1956(a)(1)(B)(i). *See United States v. Sanders*, 929 F.2d 1466, 1472 (10th Cir. 1991) (buying a car in own name or daughter's name with drug proceeds is *not* violation of (a)(1)(B)(i); § 1956 is not a "money spending" statute); *United States v. Garcia-Emanuel*, 14 F.3d 1469 (10th Cir. 1994) (simply buying horse and watch with drug proceeds and using drug proceeds to make mortgage payments insufficient to show intent to conceal or disguise); *United States v. Dobbs*, 63 F.3d 391 (5th Cir. 1995) (where SUA proceeds were deposited into wife's bank account and used for family expenses, there was insufficient evidence of intent to conceal or disguise); *United States v. Rockelman*, 49 F.3d 418, 422 (8th Cir. 1995) (defendant purchased cabin with cash and titled it in name of business, but made no attempt to hide his identity or the source of the funds). The government should prosecute transactions in which the defendant simply spends the illegally obtained proceeds as violations of § 1957.

Intent to avoid transaction reporting requirement. Finally, it is an offense to conduct a financial transaction involving SUA proceeds if the purpose

is to evade a currency transaction reporting requirement. *See* 18 U.S.C. § 1956(a)(1)(B)(ii). If, for example, a defendant evades both the Currency Transaction Report (CTR) requirement (involving $10,000 cash transactions at financial institutions) and the IRS Form 8300 requirement (involving reports that a trade or business receiving more than $10,000 in cash must file) by using a $9,000 cashier's check and $9,000 in cash to buy a car, he commits a violation of § 1956(a)(1)(B)(ii). *See United States v. Nelson*, 66 F.3d 1036 (9th Cir. 1995) (car dealer's suggestion that customer buy another car to trade-in to avoid paying more than $10,000 cash for new car shows intent to evade Form 8300); *United States v. Patino-Rojas*, 974 F.2d 94 (8th Cir. 1992) (buying cashiers' checks for $9,000 and $6,000 and giving checks and cash to dealer for $20,000 boat).

III. Section 1956(a)(2)

The elements of § 1956(a)(2)—the international money laundering statute—are the same as the elements of subsection (a)(1), with two important exceptions. First, instead of a "financial transaction," the government must show that the defendant engaged in the transportation, transfer, or transmission, of property into or out of the United States. Second, § 1956(a)(2)(A) does not contain a "proceeds" element.

A defendant violates § 1956(a)(2)(A) if he sends money into or out of the United States to promote an SUA offense, *regardless of whether the money, itself, is the proceeds of any unlawful activity.* For example, it is an offense under subsection (a)(2)(A) to send money into or out of the United States to commit bank fraud or to violate the Arms Export/Import Act or to support terrorism, even if the money is not traceable to any predicate offense. *See United States v. Piervinanzi*, 23 F.3d 670 (2d Cir. 1994) (because § 1956(a)(2)(A) contains no proceeds requirement, there is no "merger" problem when the defendant wires money out of the United States to promote fraud against a bank, and the wire transfer constitutes both the money laundering offense and the bank fraud); *United States v. Hamilton*, 931 F.2d 1046, 1052 (5th Cir. 1991) (dicta) (foreign drug cartel could violate § 1956(a)(2)(A) by sending proceeds of legitimate business into the United States for the purpose of providing necessary capital to expand cartel's United States-based drug business); *United States v. O'Connor*, 158 F. Supp. 2d 697, 726 n.52 (E.D. Va. 2001) (following *Piervinanzi*; no merger problem when defendant sends money to Bahamas and brings it back to make it appear to be new funds in furtherance of fraud scheme).

Typically, the government will establish the knowledge, proceeds, and intent elements of the offense in the same way that it would establish those elements under § 1956(a)(1). The leading case on this statute is *United States v. Cuellar*, 478 F.3d 282 (5th Cir. 2007) (en banc), in which a courier crossing the border into Mexico with drug proceeds concealed in his vehicle was convicted of transporting the proceeds with the intent to conceal or disguise. The court held that the concealment element in § 1956(a)(1)(B)(i) is the same as in § 1956(a)(2)(B)(i) (evidence that money was being transported by a low-level courier who intended to cross the border with $83,000 in currency wrapped in duct tape bundles in a hidden compartment in his vehicle was sufficient to establish that the transportation was designed to conceal; expert witness may testify that the evidence was consistent with the practice of criminals transporting illegal funds to Mexico; it was not necessary for the government to show that there was a further intent to conceal once the money arrived in Mexico); *United States* v. *Johnson*, 440 F.3d 1286, 1291 n.4 (11th Cir. 2006) (same). Accordingly, the same circumstantial evidence of concealment will support a conviction. See Figure 2, page 32.

IV. Section 1956(a)(3)

Section 1956(a)(3) was added to the money laundering statute in 1988, to make it possible to prosecute persons who engage in the laundering of "sting money," *i.e.*, money that is not really criminal proceeds but is represented as such by a law enforcement officer, or a person acting at his or her direction. In § 1956(a)(3) cases, the law enforcement officer's "representation" replaces the knowledge and proceeds elements.

Most of the litigation in sting cases involves the nature of the representation. The courts hold that what the undercover agent says to the target must convey enough information to make a reasonable person aware that the property was criminal proceeds. *See United States v. Kaufmann*, 985 F.2d 884, 892 (7th Cir. 1993) (the representation is sufficient if the law enforcement officer makes defendant "aware of circumstances from which a reasonable person would infer that the property was drug proceeds"); *United States v.*

Castaneda-Cantu, 20 F.3d 1325 (5th Cir. 1994); *United States v. Starke*, 62 F.3d 1374 (11th Cir. 1995) (same); *United States v. McLamb*, 985 F.2d 1284, 1291 (4th Cir. 1993) (representation made to car dealer sufficient where "any person of ordinary intelligence would have recognized it").

In other words, the agent does not have to come right out and say, "I'm giving you drug money to launder for me." Instead, he can imply that the money was derived from an illegal source in the vernacular of the drug trade. For example, in *United States v. Leslie*, 103 F.3d 1093, 1103 (2d Cir. 1997), the Second Circuit held that the undercover agent's statement—the cash he was giving the target was "powder-type money" that should not be brought over the border—was sufficient to allow the government to convict the target of laundering the sting money. *See also United States v. Fuller*, 974 F.2d 1474 (5th Cir. 1992) (recorded conversation in which agent describes consequences from "Colombians" if money is lost was sufficient to establish necessary representation; deliberate ignorance may satisfy knowledge requirement); *United States v. Wydermyer*, 51 F.3d 319 (2d Cir. 1995) (statement that funds to be laundered came from sale of arms smuggled into the country was sufficient to represent that property was the proceeds of a violation of the Arms Export Control Act). See Figure 3, page 33.

V. Section 1957

Section 1957 makes it an offense for any person to conduct any monetary transaction involving more than $10,000 in "criminally derived property." Its purpose is to make it difficult for wrongdoers to spend their ill-gotten gains, or to place them in the banking system, by making it a criminal offense for a third-party to do business with them. *See United States v. Rutgard*, 108 F.3d 1041, 1062 (9th Cir. 1997) (Section 1957 is designed to freeze criminal proceeds out of the banking system); *United States v. Allen*, 129 F.3d 1159, 1165 (10th Cir. 1997) (Congress's primary concern in enacting § 1957 may have been with third-parties who give criminals the opportunity to spend ill-gotten gains. Nevertheless, the statute reaches the conduct of wrongdoers who conduct transactions with the fruits of their own criminal acts.).

The government must show that more than $10,000 in SUA proceeds was involved in the transaction and that the defendant knew that the property represented the proceeds of some form of criminal activity. The government does not have to prove that the defendant acted with any specific intent. *See United States v. Abboud,* 438 F.3d 554, 594-95 (6th Cir. 2006) (unlike § 1956, § 1957 does not require proof that the transaction was intended to conceal or disguise); *United States v. Ghilarduci,* 480 F.3d 542, 551 (7th Cir. 2007) (rejecting as frivolous defendant's argument that § 1957 conviction should be reversed because there was no concealment; concealment is not an element); *United States v. Huber*, 404 F.3d 1047, 1057 (8th Cir. 2005) (§ 1956 differs from § 1957 with respect to the specific intent element; "no intent to promote or knowledge of a design to conceal is required, but the transaction must consist of property with a value greater than $10,000"); *United States v. Allen*, 129 F.3d 1159, 1165 (10th Cir. 1997) (Section 1957 proscribes a wider range of conduct than § 1956 and contains no conceal or disguise element. Thus, § 1957 applies to the most open, above-board transactions.).

Section 1957 may be used to prosecute someone for using SUA proceeds to buy a car, to invest in securities, or simply to make a deposit into a bank. *See United States v. Curry*, 461 F.3d 452, 457-58 (4th Cir. 2006) (engaging in any monetary transaction with more than $10,000 in fraud proceeds violates § 1957); *United States v. Hawkey*, 148 F.3d 920, 924 (8th Cir. 1998) (use of funds misappropriated from charitable organization to buy vehicles for personal use constituted § 1957 violation); *United States v. Kelley*, 929 F.2d 582, 585 (10th Cir. 1991) (defendant used proceeds of fraudulently obtained loan to buy car); *United States v. Taylor*, 984 F.2d 298 (9th Cir. 1993) (defendant pleads guilty to spending proceeds of wire fraud); *United States v. Cole*, 988 F.2d 681, 682 (7th Cir. 1993) (withdrawals from account containing proceeds of investment fraud scheme for personal expenses exceeding $10,000); *United States v. Hollis*, 971 F.2d 1441, 1446-47 (10th Cir. 1992) (deposit of checks representing proceeds of insurance fraud scheme is a § 1957 violation); *United States v. One 1987 Mercedes Benz 300E*, 820 F. Supp. 248 (E.D. Va. 1993) (purchase of car with check drawn on account into which extortion proceeds had previously been deposited).

Despite some difference in wording, the knowledge element in § 1957 is the same as it is for a § 1956 offense: the defendant must know that the property was derived from some form of

unlawful activity. *See United States v. Turman*, 122 F.3d 1167 (9th Cir. 1997) (government must prove the defendant knew property was criminally derived, but does not have to prove the defendant knew money laundering itself was illegal); *United States v. Sokolow*, 81 F.3d 397 (3d Cir. 1996) (defendant does not need to know that the monetary transaction constitutes a criminal offense); *United States v. Smith*, 44 F.3d 1259 (4th Cir. 1995) (knowledge that the property is criminally derived is all that is required; defendant need not know that the transaction was part of a larger scheme to conceal or disguise anything); *United States v. Campbell*, 977 F.2d 854 (4th Cir. 1992) (real estate agent doing business with drug dealer can be convicted under § 1957, if the agent knows of, or is willfully blind to, customer's source of funds); *United States v. Wynn*, 61 F.3d 921, 927 (D.C. Cir. 1995) (same for merchant selling clothes to drug dealer).

In § 1957, the phrase "criminally derived property" means the same thing as § 1956's "proceeds of specified unlawful activity": the property must be the proceeds of an SUA at the time the transaction takes place. *See United States v. Savage*, 67 F.3d 1435 (9th Cir. 1995). The important limitations in § 1957 are that the transaction must be conducted by, to, or through, a financial institution, and it must involve more than $10,000 in SUA proceeds.

In most cases, the financial institution requirement is easily met because the term "financial institution" includes not only banks and other traditional institutions, but also any other type of entity listed in 31 U.S.C. § 5312, or the regulations promulgated thereunder. Thus, the definition of "financial institution" is very broad and includes car dealers, jewelers, attorneys handling real estate closings, and even individuals, if they handle currency on a regular basis to provide services to others. *See United States v. Pizano*, 421 F.3d 707, 713 (8th Cir. 2005) (down payments on real property made with check and wire transfer were monetary transactions); *United States v. Dazey*, 403 F.3d 1147, 1163 (10th Cir. 2005) (cashing a check is a monetary transaction); *United States v. Huber*, 404 F.3d 1047, 1060 n.8 (8th Cir. 2005) (using a check is monetary transaction; transaction must be "by, through or to a financial institution"); *United States v. Tannenbaum*, 934 F.2d 8 (2d Cir. 1991) (an individual can be a financial institution).

The key issue in most § 1957 cases is the $10,000 threshold requirement. Because each monetary transaction is a separate offense, it is generally not possible to aggregate separate transactions to reach the $10,000 threshold. Multiple purchases from the same vendor on the same day, or installment payments on the same item, may, however, constitute a single transaction in some circumstances. *See United States v. George*, 363 F.3d 666, 674-75 (7th Cir. 2004) (purchasing car with cash in two installments of $6,000 and $9,000 satisfies the $10,000 requirement). The question seems to be one for the jury to decide. *See United States v. Caldwell*, 302 F.3d 399, 406 (5th Cir. 2002) (noting that district court set aside jury's verdict on one § 1957 count on ground that the amount could not be aggregated; no government appeal); *United States v. Brown*, 139 F.3d 893 (4th Cir. 1998) (Table Case) (whether purchase of several automobiles on same day from same vendor constituted single monetary transaction exceeding $10,000 was question for jury).

A related issue arises when the defendant commingles the SUA proceeds in a bank account and then makes a withdrawal that the government wants to charge as a violation of § 1957. The government generally takes the view that, as long as more than $10,000 in SUA proceeds was deposited into the account, any subsequent withdrawal of more than $10,000 may be said to involve the requisite amount of tainted funds. In *United States v. Rutgard*, 108 F.3d 1041, 1063 (9th Cir. 1997), however, the court held that the defendant is entitled to a presumption that the tainted money remains in a bank account until the last withdrawal. Thus, if the defendant puts $50,000 in illegal proceeds into a bank account containing $10,000 in "clean" money, and then makes a $15,000 withdrawal, the Ninth Circuit would likely hold that this does not satisfy the threshold requirement for § 1957. Because of the "last out" rule, courts in the Ninth Circuit must presume that the $15,000 withdrawal consisted primarily of the clean money, while the "dirty" money remained in the bank account. The courts are generally split on this issue. *See United States v. Davis*, 226 F.3d 346, 357 (5th Cir. 2000) ("when the aggregate amount withdrawn from an account containing commingled funds exceeds the clean funds, [any] individual withdrawal[s] may be said to be of tainted money, even if a particular withdrawal was less than the amount of clean money in the account"); *United States v. Haddad*,

462 F.3d 783, 792 (7th Cir. 2006) (where the "vast majority" of funds in a commingled account containing $18,000 is fraud proceeds, the evidence is sufficient to prove that more than $10,000 of a $16,000 withdrawal was fraud proceeds; rejecting *Rutgard*); *United States v. Mooney*, 401 F.3d 940, 946 (8th Cir. 2005) (deposit of five checks drawn on an account containing commingled funds was a § 1957 offense even though there was enough clean money in the account to cover the checks; "the government need not trace each dollar to a criminal source to prove a violation of 18 U.S.C. § 1957"); *United States v. Johnson*, 971 F.2d 562, 570 (10th Cir. 1992) (in the context of a withdrawal, the government is not required to prove that no untainted funds were commingled with the unlawful proceeds for § 1957 purposes). See Figure 4, page 33.

VI. Comparison of Sections 1956 and 1957

Section 1956	Section 1957
Twenty year felony	Ten year felony
Financial transaction (interstate commerce)	Monetary transaction (requires use of financial institution)
Knows some form of felonious conduct	Knows criminally derived property
No $ threshold	Greater than $10,000
Sting provision	No sting provision
Specific intent	No specific intent
No Sixth Amendment exclusion	Excludes transaction necessary to protect Sixth Amendment rights

VII. Conspiracy

Section 1956 and 1957 offenses may be alleged as objects of a conspiracy under 18 U.S.C. § 371. This is useful where the government wants to charge money laundering, along with other offenses, in a multiobject conspiracy. Keep in mind that the court must instruct the jury that it must be unanimous as to which offense(s) were the object of the conspiracy. *See United States v. Nattier*, 127 F.3d 655 (8th Cir. 1997).

Most money laundering conspiracies are charged under 18 U.S.C. § 1956(h), however. This is the preferred method of charging for several reasons. First, unlike § 371, there is no overt act requirement under § 1956(h). *See Whitfield v. United States*, 543 U.S. 209, 211 (2005). Second, the maximum penalty for a § 1956(h) conspiracy is the same as the penalty for the offense that is the object of the conspiracy, i.e., twenty years for a § 1956 offense, and ten years for a § 1957 offense. *See United States v. Abrego*, 141 F.3d 142 (5th Cir. 1998) (higher penalty under § 1956(h) applies to "straddle" conspiracies; no violation of *ex post facto* clause). This contrasts with the five-year maximum penalty for § 371 conspiracies outside of the Fifth Circuit. Lastly, unlike § 371 prosecutions, property involved in a § 1956(h) conspiracy is subject to forfeiture under 18 U.S.C. § 982(a)(1).

VIII. Resources

The Asset Forfeiture and Money Laundering Section (AFMLS) publishes an annual collection of all relevant federal cases in a bound volume entitled "Federal Money Laundering Cases." Copies are available to United States Attorneys' offices. Call the AFMLS at (202) 514-1263, to request copies. Finally, AFMLS maintains AF Online, a computer-based legal resource from which we can access a collection of cases, form indictments and jury instructions, and other materials. Contact Beliue Gebeyehou at (202) 307-0265, for help accessing AF Online.❖

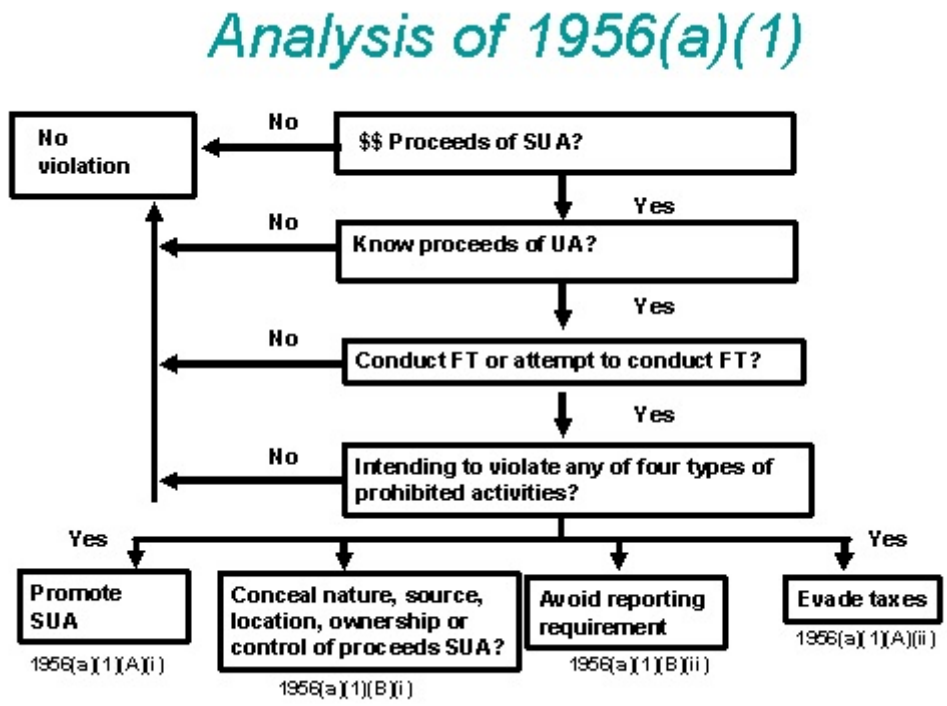

Figure 1

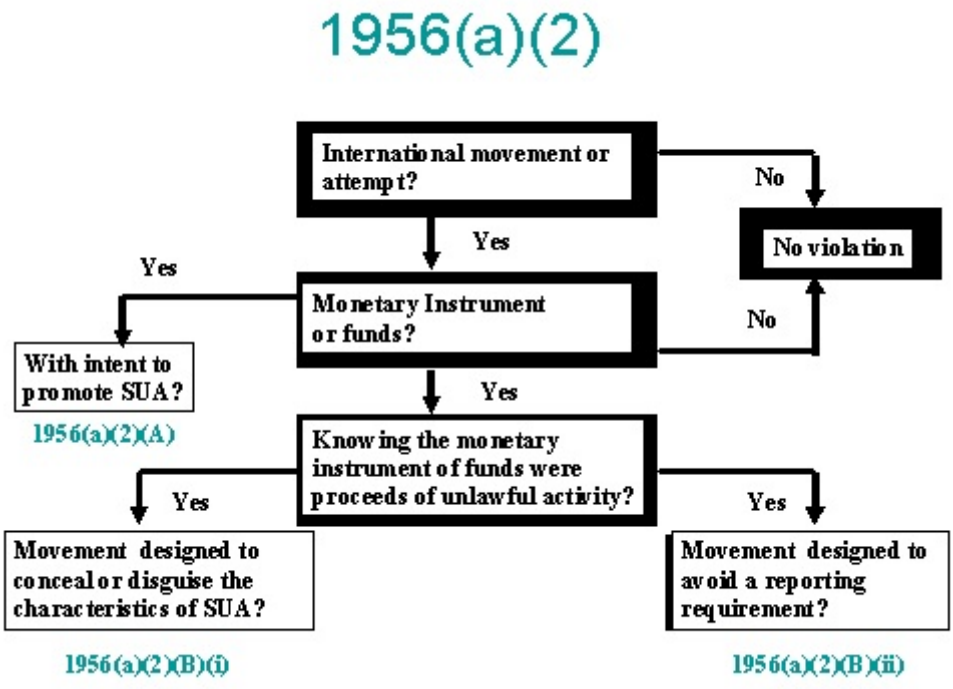

Figure 2

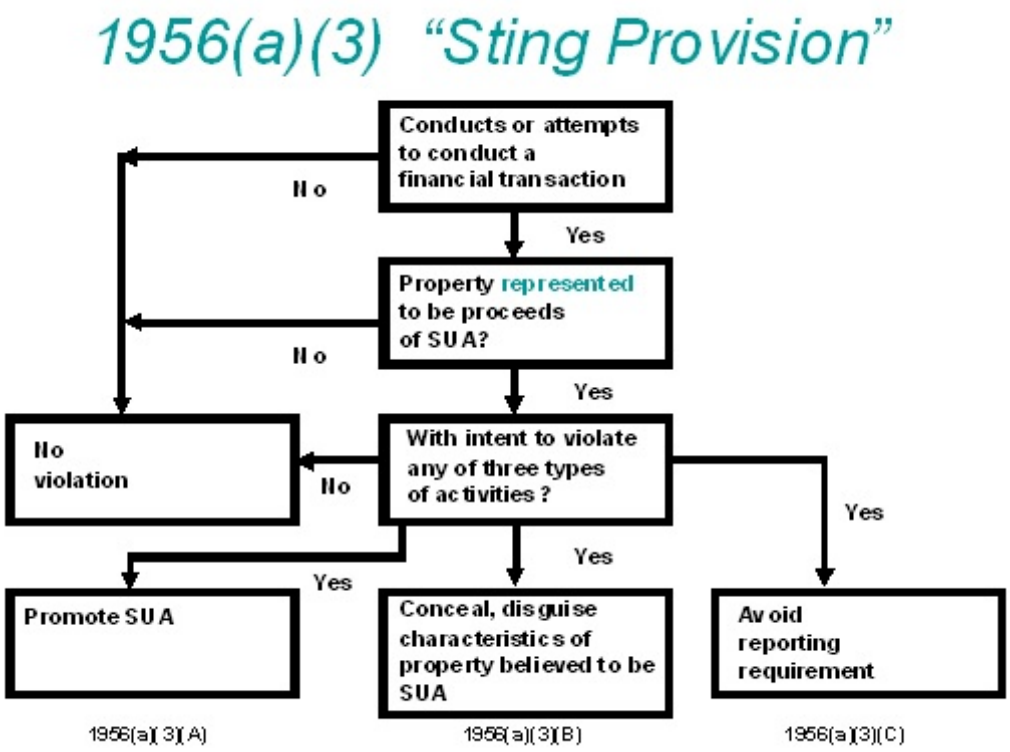

Figure 3

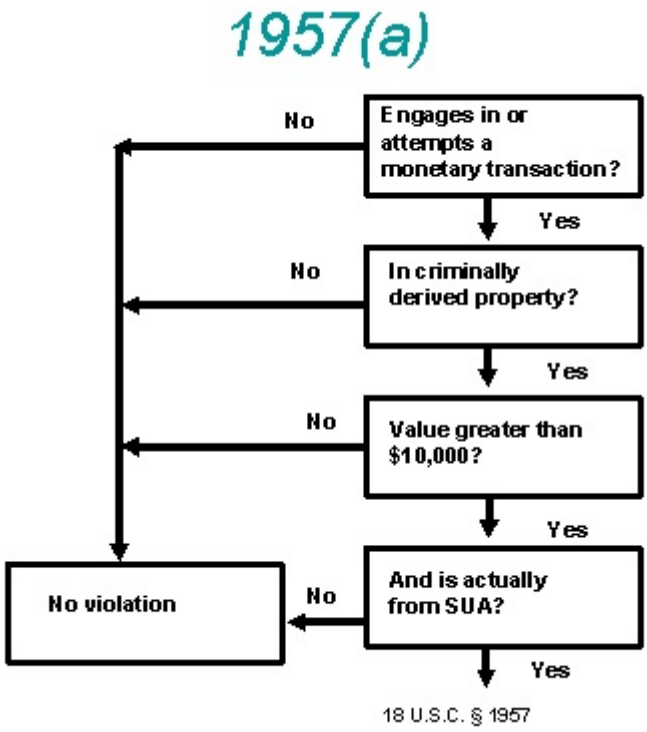

Figure 4

ABOUT THE AUTHOR

❑**Stefan D. Cassella** is the Deputy Chief for Legal Policy in the Asset Forfeiture and Money Laundering Section. He has been a prosecutor since 1979. He came to the Department of Justice in 1985 and has been involved in forfeiture and money laundering issues since 1989. He handles civil and criminal forfeiture cases, lectures at training conferences on many aspects of money laundering and forfeiture law, and is responsible for legal advice, policy, and legislative issues for the Department. He has published numerous law review articles on forfeiture, a treatise entitled *Asset Forfeiture Law in the United States,* and is the editor of *Quick Release*, the Department's forfeiture newsletter. From 1987-89, he served as Senior Counsel to the U.S. Senate Judiciary Committee.✠

One-Hour Money Laundering: Prosecuting Unlicensed Money Transmitting Businesses Using Section 1960

Courtney J. Linn
Assistant United States Attorney
Eastern District of California

I. Introduction

Section 1960 of Title 18 makes it a crime to conduct an unlicensed money transmitting business. Congress enacted the statute fifteen years ago amid concerns that money transmitting businesses facilitated money laundering. These concerns persist. According to the 2005 National Money Laundering Threat Assessment and the 2007 National Drug Threat Assessment, money transmitters continue to provide a conduit for money launderers, particularly those linked to narcotics trafficking. These assessments led to the call, in the 2007 National Money Laundering Strategy, for the law enforcement community to continue to "work aggressively to identify and prosecute [money transmitting businesses] that facilitate money laundering." *Available at* http://www.treas.gov/press/releases/docs/nmls.pdf.

Given these threats, it is somewhat surprising to learn that prior to the passage of the USA PATRIOT Act, there was only one reported § 1960 case. *See United States v. Velastegui*, 199 F.3d 590, 593 (2d Cir. 1999). With the benefit of hindsight, it is easy to understand why prosecutors so seldom used § 1960. First, in its original form, § 1960 made it a crime to conduct a money transmitting business in a state that imposed a licensing requirement, and punished the lack of a license as either a misdemeanor or a felony. Unfortunately, during the 1990s, many states were just beginning to impose a licensing requirement on money transmitters and/or enacting criminal penalties. Second, in 1994, Congress amended § 1960 to add a second prong. This added prong

made it a crime to conduct a money transmitting business that failed to register with the Financial Crimes Enforcement Network (FinCEN), a bureau of the Department of Treasury. However, the provision required the drafting of implementing regulations. Third, prior to amendments to the statute in the USA PATRIOT Act, questions existed about the statute's *mens rea* element, particularly under the state licensing prong. If, as one district court held, the state licensing prong required proof that the person conducting the business knew of the state licensing requirement, and knew the state punished the operation of the unlicensed business as a crime, it would prove difficult indeed to obtain a § 1960 conviction.

By late 2001, all three of these issues had been resolved. A large number of states enacted licensing requirements enforced by felony or misdemeanor punishments in the years between 1992 and 2001, and regulations that gave effect to the 1994 federal registration requirement became operative in 1999. *See* 31 C.F.R. 103.41 (effective August 20, 1999). In the USA PATRIOT Act, Congress clarified the statute's mens rea requirement.

Following these legislative and regulatory changes, we have seen a sharp increase in the number of § 1960 prosecutions and convictions. In Fiscal Year (FY) 2001 (which ended just prior to the passage of the USA PATRIOT Act), prosecutors filed § 1960 charges against ten defendants. In FY 2006, in contrast, prosecutors filed § 1960 charges against 107 defendants. Reported judicial decisions mirror this trend. Since 2001, there have been approximately thirty-five reported judicial decisions.

In short, § 1960 is only now emerging as an effective tool to address the money laundering threats posed by money transmitting businesses. The statute's increased use makes this a good time to examine it.

II. Legislative history

There is remarkably little legislative history supporting the enactment of § 1960. The Annunzio-Wylie Money Laundering Act, Pub. L. No. 102-550, 106 Stat. 4044 (1992) (of which § 1960 was part) was a last-minute conference addition to the Housing and Community Development Act of 1992, Pub. L. No. 102-550, 106 Stat. 3672 (1992). Nonetheless, a more complete explanation of the purpose of the statute appears in the report of the Senate Banking Committee in the prior session of Congress. *See* S. REP. NO. 101-460 (1990). Though legislative history issued in connection with an unenacted version of a statute is not a secure indicator of congressional intent (*Ratzlaf v. United States*, 510 U.S. 135, 148 n.18 (1994)), it nonetheless sheds some light on the statute's intended scope and meaning.

First, the legislative history indicates that Congress modeled the statute after the illegal gambling business statute, 18 U.S.C. § 1955. S. REP. NO. 101-460, at 14 (1990). Prior to § 1960's enactment, the Supreme Court had definitively interpreted § 1955. *See Sanabria v. United States*, 437 U.S. 54 (1978). Thus, the construction that the Supreme Court placed on § 1955 should guide courts when construing the nearly identical language in § 1960. *See United States v. Wells*, 519 U.S. 482, 495 (1997) (if the Supreme Court has already provided a definitive interpretation of the language in one statute, and Congress then uses nearly identical language in another statute, a court should give the language in the latter statute an identical interpretation, unless there is a clear indication in the text or legislative history that it should not do so).

Second, Congress seems to have intended § 1960 to reach only a comparatively small segment of the nonbank financial services industry. In congressional hearings in the session preceding the enactment of § 1960, Congress heard testimony about the threats posed by different kinds of nonbank financial services activity, including money transmitting, currency exchanging, and check cashing. But its attention was particularly drawn to money transmitters. *See, e.g.,* S. REP. NO. 101-460, at 14 (1990).

> As banks became more sophisticated in reporting currency transactions, drug dealers became more creative and began to rely increasingly on unlicensed and illegal money transmitters, on check cashers, and on money order vendors, all users and sources of high amounts of cash * * * It is primarily the unlicensed money transmitter that provides the best means of laundering money and is most often used to structure illegal transactions) (emphasis added).

See also United States v. Velastegui, 199 F.3d 590 (2d Cir. 1999). As discussed below, this legislative history, coupled with the somewhat narrow definition of "money transmitting" in § 1960(b)(2), may indicate that check cashers and

currency exchangers fall outside of § 1960's ambit.

Finally, the legislative history reveals that when Congress amended § 1960 in the USA PATRIOT Act, it understood the statute to reach not just storefront money transmitters, but also informal value transfer systems through which criminals transmit money, such as hawalas and the cash courier operations of drug traffickers. *See* H.R. REP. NO. 107-250, at 54 (2001) ("Thus, a person who agrees to transmit or to transport drug proceeds for a drug dealer, or funds from any source for a terrorist, knowing such funds are to be used to commit a terrorist act, would be engaged in the operation of an unlicensed money transmitting business.") Here, we need to be cautious about giving too much weight to the legislative history because these statements occurred years after § 1960's passage. *Oscar Mayer & Co. v. Evans*, 441 U.S. 750, 758 (1979). That said, the statements provide some support for the conclusion that § 1960's definition of "money transmitting" is flexible and expansive enough to encompass at least some nonbank financial services activity, such as web-based value transfer schemes.

III. Elements of the statute

Section 1960 makes it illegal to knowingly conduct, control, manage, supervise, direct, or own all or part of an unlicensed money transmitting business. 18 U.S.C. § 1960. The statute defines three alternative forms of an "unlicensed money transmitting business." A money transmitting business is unlicensed if it affects interstate or foreign commerce and: (1) operates without an appropriate money transmitting license in a state where such operation is punishable as a misdemeanor or felony, § 1960(b)(1)(A); (2) fails to comply with the money transmitting business registration requirements under section 5330 of Title 31 and the implementing regulations, § 1960(b)(1)(B); or (3) involves the transportation or transmission of funds that are known to the defendant to have been derived from a criminal offense or are intended to be used to promote or support unlawful activity, § 1960(b)(1)(C).

The state licensing and federal registration prongs have comparable elements. The government must prove: (1) the defendant knowingly conducted a money transmitting business; (2) the business affected interstate or foreign commerce; (3) the business was unlicensed under state law [or failed to register under federal law]; (4) the state [or federal government] required a license [or registration]; and (5) in the case of the state licensing prong, state law punished the lack of a license as a misdemeanor or felony.

To date, virtually all known § 1960 prosecutions have been brought under either the state licensing or federal registration prong, and thus the elements of those prongs are discussed in greater detail below. The third prong—what might be termed the "money laundering/reverse money laundering prong" because it resembles a money laundering statute–has not received much attention.

A. Defendant knowingly conducts, controls, manages, supervises, directs, or owns a money transmitting business

Knowingly. In the wake of the Supreme Court's 1994 decision in *United States v. Ratzlaf*, 510 U.S. 135 (1994), a concern arose that courts would construe the former "intent" element in the state licensing prong of § 1960 to require proof that defendant knew of the state licensing requirement and that state law punished it as a misdemeanor or felony. In the USA PATRIOT Act, Congress addressed this concern. It amended the state licensing prong of § 1960 to eliminate the "intent" element. As if to put an exclamation point on this deletion, Congress added language in the statute making it clear that the state licensing prong is violated "whether or not the defendant knew that the operation was required to be licensed or that the operation was so punishable." 18 U.S.C. § 1960(b)(1)(A). Judicial decisions have now confirmed that neither the state licensing prong nor the federal registration prong of § 1960 requires proof that the defendant knew of the licensing or registration requirements or knew of the consequences of the failure to license or register. *See, e.g.*, *United States v. Talebnejad*, 460 F.3d 563, 568-70 (4th Cir. 2006), *cert. denied*, 127 S. Ct. 1313 (2007); *United States v. Keleta*, 441 F. Supp. 2d 1 (D.D.C. June 28, 2006); *United States v. Uddin*, 365 F. Supp. 2d 825 (E.D. Mich. 2005).

Conducts, controls, manages, supervises, directs, or owns. The statute's licensing and registration prongs do not punish "money transmitting" per se, and they do not punish the existence of an unlicensed money transmitting

business. Instead, § 1960 makes it a crime to conduct, control, manage, supervise, direct, or own an unlicensed money transmitting business. *Sanabria v. United States*, 437 U.S. 54, 70 (1978) (allowable unit of prosecution under § 1955 is participation in a single illegal gambling business; Congress did not define discrete acts of gambling as independent federal offenses). Significantly, the Supreme Court explained in *Sanabria* that § 1955 proscribes any degree of participation in the illegal gambling business (except by mere bettors). *See Sanabria,* 437 U.S. at 70-71 and n.26. Thus, we would have expected courts to construe § 1960 similarly to reach all participants in the business, except customers. However, without addressing *Sanabria*, the Fourth Circuit in *Talebnejad*, construed the language "conducts, controls, manages, supervises, directs, or owns" to mean that "[c]riminal liability is... directed toward those who are, in some substantial degree, in charge of the operation; the statute does not reach mere employees." 460 F.3d at 272. This construction of § 1960 is difficult to reconcile with *Sanabria*, which construed the almost identical terminology much more broadly, especially given that Congress modeled § 1960 after the very statute the Supreme Court construed in *Sanabria*. Nonetheless, unless overruled, the *Talebnejad* decision may restrict the government's ability in the Fourth Circuit to charge culpable employees (and perhaps even passive owners) of the money transmitting business under the state licensing and federal registration prongs.

Money transmitting. As discussed above, § 1960(b)(2) defines "money transmitting" to include transfers of funds on behalf of the public by any and all means, including, but not limited to, transfers within this country or to locations abroad by wire, check, draft, facsimile or courier. In an ordinary sense, the term "transfer" means to move or send money to a different location. *See* Webster's Third New Int'l Dictionary 2427 (1993). This definition–considered in the context of the legislative history discussed above–gives reason to doubt whether check cashing, currency exchanging, and similar activities come within the ambit of § 1960. Neither a check cashing business nor a currency exchange business moves or sends money from one location to another, so much as they exchange one form of currency for another, or exchange a check for currency. That said, the term "transfer" in § 1960(b)(2) appears to be broad enough to encompass hawala and other alternative-value type transfer activities in which funds do not physically, or even electronically, move in the transaction. *Cf. United States v. Dinero Express, Inc.*, 313 F.3d 803, 806 (2d Cir. 2002) ("Because money is inherently fungible, a person is sensibly considered to have engaged in a 'transfer' of money whenever he accepts money in one location and, pursuant to an overall course of conduct, causes the delivery of related money to another location."); *see also* Stefan D. Cassella, *Application of Section 1960 to Informal Money Services Businesses*, Criminal Law Bulletin 590 (West, Sept.-Oct. 2003).

Business. The statute requires proof of an unlicensed money transmitting *business*. The business requirement ensures that persons cannot be convicted for a single, isolated instance of improper transmittal of money not shown to be part of a business. *United States v. Velastegui*, 199 F.3d 590, 595 n.4 (2d Cir. 1999). Embedded in the definition of "money transmitting" is a similar restriction. That definition specifies that money transmitting includes transfers conducted "on behalf of the public," suggesting that the remittance activity must be conducted on behalf of a third person or persons. These two requirements, *i.e.*, the requirement that the government prove the existence of a business, and prove that the funds were transferred on behalf of the public, may therefore preclude prosecution of an isolated instance of money transmitting and of transmissions conducted on behalf of oneself.

Proof of the existence of a business may take many forms. Proof may come in the form of ledgers and receipts documenting money transmission on behalf of third persons. It may also take the form of representations made through advertisements, through applications for general business permits, and through representations made in account opening documents maintained by banks handling the money transmitter's transactions.

B. Affects interstate or foreign commerce

The second element of the statute requires proof that the business affects interstate or foreign commerce in any manner or degree. In most cases, the money transmitting business either directly transmits funds in interstate or foreign commerce, or uses a financial intermediary, *e.g.*, a federally-insured bank, to do so. In either case, proof that the business engages in transactions in interstate or foreign commerce will satisfy the interstate commerce element. *See, e.g., United States v. Oliveros*, 275 F.3d 1299, 1304 (11th Cir. 2001)

(handing over a check implicates interstate commerce if subsequently the check is deposited in a bank; bank's involvement can be incidental and need not be integral to the particular transaction charged as money laundering). In the case of a hawala-type transfer system that operates entirely outside the financial system, proof may take the form of interstate or transnational communications between hawaladars.

C. The business is unlicensed under state law [or fails to register under federal law]

The *Talebnejad* decision tells us that the statute's mental state requirement (knowledge) applies to the first three elements of the offense, that is, the factual elements. The knowledge requirement does not apply to the last two elements, the legal elements. This means that the government must prove that the defendant charged with conducting the unlicensed money transmitting business knew that the business lacked the requisite license and/or registration, even though the government does not have to prove that the defendant knew about the licensing and/or registration requirement. Apart from raising an interesting metaphysical question–can someone know that he or she lacks a license without knowing of the licensing requirement–the knowledge requirement may leave room for a defendant to offer an objective mistake-of-fact defense. Arguably, for example, it is a defense to a § 1960 charge if the defendant establishes an objectively reasonable, but mistaken belief that his or her business partner had secured the requisite license and/or registration. It is not, however, a defense that the defendant subjectively, but unreasonably believed, for example, that a business permit sufficed to operate a money transmitting business, or mistook the law, or received bad legal advice. *See, e.g., United States v. Cross*, 113 F. Supp. 2d 1253, 1256, 1262 (S.D. Ind. 2000) (because offense of operating an illegal gambling business was a general intent crime, advice of counsel was unavailable as a defense to that crime).

D. The state [or federal government] requires a license [or registration]

State licensing requirements. FinCEN maintains a list of states that have enacted some form of licensing requirement for money transmitting businesses. *See* http://www.msb.gov/pdf/msbstatecontactsfinal.pdf. Care should be taken in reading these state licensing provisions. Some states, for example, impose licensing requirements, but only for businesses engaged in international money transmitting. *See, e.g.*, Cal. Fin. Code § 1800.5; *see also* Mass. Gen. L. Ch. 169, § 16; N.J. Rev. Stat. § 17:15C-2. Other states may define the licensing requirement in terms that reach only money transmission activities that occur within the state. *See, e.g.*, *United v. Bah*, 2007 WL 1032260 (S.D.N.Y. Mar. 30, 2007) (collecting money in New York for transmission, where transmission activity itself occurs in New Jersey, does not implicate New York's money transmitter licensing requirement).

The federal registration requirements. Law enforcement agents and prosecutors should exercise special caution when investigating and prosecuting a case under the federal registration prong of § 1960. The federal registration regulations contain ambiguities and exceptions. *See FinCEN and IRS Need to Improve and Better Coordinate Compliance and Data management Efforts*, GAO-07-212 at 12 (Dec. 2006) (characterizing the regulations as "confusing and easily misinterpreted"). To begin, the regulations do not use the term "money transmitting business," even though that is the term Congress used in both § 1960 and in 31 U.S.C. § 5330, the statute creating the federal registration requirement. The regulations instead introduce a term alien to the statutory scheme, "money services business." In addition, the regulations carve up the registration requirement with numerous exceptions. For example, money transmitters that merely act as an agent of a registered money transmitter do not have to register with FinCEN. *See* 31 C.F.R. § 103.41(a)(2) (2006). These exceptions, particularly the agency exception, have made it difficult for law enforcement agencies, money transmitting business examiners, and banks, to identify whether a money transmitter is subject to the registration requirement.

If § 1960 applied to other forms of money services businesses other than money transmitters, *e.g.*, check cashers, then the regulatory framework becomes even more complicated. Some money services businesses (*i.e.*, issuers and redeemers of stored value) have been completely exempted from the registration requirement (31 C.F.R. § 103.41(a)(2)), while others (*e.g.,* check cashers) qualify as a money services business only if they handle more than a $1,000 on behalf of a single customer in a single day. *See* 31 C.F.R. § 103.11(uu)(1)-(4).

E. State law punishes the lack of a license as a misdemeanor or felony

The requirement that the state punish the offense as either a misdemeanor or felony may raise legal issues in at least two contexts. The first context is where the state attaches misdemeanor or felony penalties only upon proof that a defendant "willfully" or "intentionally" violated the state statute, *i.e.*, proof that the defendant knew of the licensing requirement. The *Talebnejad* court ruled that Congress expressly rejected any mens rea requirement with respect to the legal elements of the state licensing prong of § 1960. 460 F.3d at 567.

The other context in which this element may give rise to a legal issue is where the state statute proscribes misdemeanor or felony penalties, but only if a statutory precondition has been met. In California, for example, unlicensed check cashers are subject to misdemeanor penalties, but only if they have first been cited for infractions. *See* Cal. Civ. Code § 1789.37 (West 2006). If state law provided for such a precondition to misdemeanor or felony punishment, it is likely the government would have to prove the precondition to satisfy this element of the statute, because otherwise the operation of the money transmitting business would not be "punishable" as a misdemeanor or felony under state law.

IV. Constitutional challenges and defenses

The courts have, thus far, addressed numerous constitutional challenges to § 1960, and rejected them. Some defendants have raised equal protection challenges to the state licensing prong. They have challenged § 1960 on the ground that it violates the Equal Protection Clause because it assimilates the laws of some states, but not others. These challenges have been uniformly rejected. *See, e.g.*, *United States v. Barre*, 324 F. Supp. 2d 1173, 1175-76 (D. Colo. 2004). Other challenges, premised on fair notice, vagueness, and the rule of lenity, have similarly been rejected.

Perhaps the most serious constitutional challenge is the one raised in *Talebnejad*, 460 F.3d 563, 570. There, the defendants argued that § 1960's comparatively low mental state requirement violated due process, citing *United States v. Lambert*, 355 U.S. 225 (1957) (striking down municipal ordinance that required a convicted felon to register with the city, and subjected the felon to criminal penalties, even if he or she was unaware of the registration requirement). The *Talebnejad* Court distinguished *Lambert*. Unlike the situation in *Lambert*, which involved wholly passive conduct, § 1960 criminalizes affirmative conduct, *e.g.*, the conduct or operation of an unlicensed money transmitting business. Judge Gregory, in his partial dissent, left room for the possibility that § 1960 might be susceptible to an as-applied constitutional challenge if the government used § 1960 to prosecute, for example, a passive or minority stakeholder in a money transmitting business. Such facts would, in Judge Gregory's view, resemble those in *Lambert,* and thus raise concerns about whether the statute provided constitutionally sufficient notice of possible regulation. 460 F.3d at 576.

V. Sentencing and forfeiture

Sentencing. The Sentencing Commission has placed § 1960 violations in two different sections of the Guidelines, depending on which prong forms the basis for the conviction. The Commission analogized violations of the state licensing and federal registration prongs of § 1960 to currency reporting offenses, and thus classified those offenses under USSG § 2S1.3. *See* Appendix C, amendment 634. However, the Sentencing Commission analogized violations of the proceeds/reverse money laundering prong of § 1960 to a money laundering offense, and assigned it to USSG § 2S1.1. *See* Appendix C, Amendment 655.

The Sentencing Commission's bifurcated treatment of § 1960 may lead to sentencing anomalies. A money transmitter that violates the state licensing or registration prongs will be sentenced based on the total amount of funds transmitted, without regard to whether those funds derived from a criminal source or were intended for a criminal purpose. *See United States v. Bariek*, 2005 WL 2334682 at *2 (E.D. Va. Sept. 23, 2005) (because § 1960 was enacted to prevent terrorists, money launderers and other criminals from exploiting unregulated banking systems, the more money transmitted by an unlicensed business, the more likely that some of that money will find its way into criminal hands, and the greater harm caused; it is thus appropriate to reach a sentencing range determination based on the amount transmitted). However, a defendant sentenced under the money laundering/reverse money laundering prong of § 1960 will be

sentenced based only on the total amount of the funds involved in the particular money laundering/reverse money laundering transactions–a figure that may represent just a small fraction of the total amount transmitted through the business.

In the case of violations of the licensing and registration prongs, defendants have variously argued that USSG § 2S1.3(a) overstates the seriousness of the § 1960 offense, and some of these arguments have begun to gain traction in the courts. For example, one defendant has successfully argued, in a case based on a § 1960 violation of Virginia's state licensing requirement, that the sentencing judge should take into account the sentence that the defendant likely would have received for the state law violation had he been prosecuted in Virginia state court. S*ee United States v. Habbal*, 2005 WL 2674999 at *4 (E.D. Va. Oct. 17, 2005) (in case where defendant violated Virginia state licensing requirement, but complied with federal registration requirement, court took into account sentence defendant would have faced if prosecuted in state court for licensing offense); *United States v. Clark*, 434 F.3d 684 (4th Cir. 2006) (Motz, J., dissenting).

Defense attempts to qualify for a reduced advisory guideline range under the § 2S1.3(b)(2) safe harbor provision have been less successful. To qualify, money transmitters would have to show, among other things, that the funds they transmitted on behalf of their customers derived from a lawful source and were intended for a lawful purpose. In most cases with a probable or even possible money laundering nexus, the money transmitters will be unable to make that showing because he or she will not be able to establish that the customers of the money transmitter derived their funds from legitimate sources. *United States v. Abdi*, 342 F.3d 313 (4th Cir. 2003).

Forfeiture. Federal law subjects all property, real or personal, involved in a transaction or attempted transaction in violation of § 1960, or any property traceable to such property, to civil and criminal forfeiture. This means that the forfeiture may include all property involved in the operation of the money transmitting business itself, including its business assets. *See* Stefan D. Cassella, *Asset Forfeiture Law in the United States*, § 27-5 (JurisNet 2007). It also means that the forfeiture may include the funds being transmitted by a money transmitter who is acting in violation of the statute. *Id*.

The potential breadth of forfeiture under § 1960 may give rise to two issues. First, an issue may arise whether customers of an unlicensed money transmitting business have standing to contest the forfeiture of funds seized from the business, when those funds are linked to transactions the customers initiated through the business. *See, e.g.*, *United States* v. *47-10-Ounce Gold Bars*, No. CV 03-955-MA, 2005 WL 221259 (D. Ore. Jan. 28, 2005). Second, in cases prosecuted under the state licensing and federal registration prongs, claimants and defendants may raise an excessive fines defense comparable to that which was raised *in United States v. Bajakajian*, 524 U.S. 321, 326 (1998). *Bajakajian* is distinguishable. Unlike *Bajakajian*, which involved a one-time failure to file a report, a violation of the state licensing and registration prongs necessarily involves at least an ongoing failure to act. *Cf. United States v. Wallace*, 389 F.3d 483, 487 (5th Cir. 2004) ("Obviously, he was operating an unregistered airplane on an ongoing basis, as opposed to the one time violation in *Bajakajian*"). Moreover, cases prosecuted under the money laundering/reverse money laundering prong of § 1960 are even less likely to raise Excessive Fines Clause issues because the Excessive Fines Clause has no application to the forfeiture of crime proceeds.

VI. Conclusion

Section 1960 is an extraordinarily powerful statute—one that greatly enhances the government's ability to combat drug money laundering and terrorist financing. However, because of the interplay between the statute, state law, and federal regulations, § 1960 can be a difficult statute to use in practice. Prosecutors are encouraged to contact the Asset Forfeiture and Money Laundering Section when considering a prosecution or forfeiture under this statute.❖

ABOUT THE AUTHOR

❑**Courtney J. Linn** is an Assistant U.S. Attorney in the Eastern District of California, and wrote this article while on detail this past year to the Asset Forfeiture and Money Laundering Section of the Criminal Division. A longer version of this article will appear later this year in the UC Davis Business Law Journal. *See* http://blj.ucdavis.edu. The author and the Office of Legal Education thank the UC Davis Business Law Journal for allowing this digest version of the article to be made available to prosecutors prior to the article's publication.✠

Bulk Cash Smuggling

Rita Elizabeth Foley
Assistant United States Attorney
Eastern District of Michigan

I. Introduction

Google the phrase "bulk cash smuggling" and, in less than one second, more than 11,000 search results will pop up. Many of those hits will, in some way, reference Title 31 of the United States Code, specifically Section 5332, which is often referred to as the Bulk Cash Smuggling Act of 2001. The criminalization of bulk cash smuggling clearly gained sudden impetus following 9/11. The Bulk Cash Smuggling Act was reintroduced in the House of Representatives as a bill, H.R. 2920, 107th Cong. (2001), on September 20, 2001. Section 5332 of Title 31 of the United States Code was enacted on October 26, 2001 as part of the USA PATRIOT ACT (Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism Act [USA PATRIOT ACT] of 2001), USA PATRIOT ACT, Pub. L. No. 107-56, Tit. III, § 371, 115 Stat. 272 (2001).

The initial push to heighten awareness of bulk cash smuggling as a serious offense, however, came in 1998, as the government responded to the decision of the United States Supreme Court in *U.S. v. Bajakajian*, 524 U.S. 321 (1998). The *Bajakajian* decision has been reviewed and discussed at length since its issue. In short, the Supreme Court held that forfeiture of the entire amount of $357,144 in U.S. currency seized from Mr. Bajakajian was excessive. The Court reasoned that, since the wrongful act was a mere failure to file a report in violation of 31 U.S.C. § 5316, forfeiture of the entire amount of the seized currency was grossly disproportional to the gravity of the offense, and violated Mr. Bajakajian's Eighth Amendment right to be protected from excessive fines. Ultimately, the Court ruled that Mr. Bajakajian only had to forfeit $15,000 of the $357,144 in currency.

II. Legislative history

In 1998, following the *Bajakajian* decision, the United States Department of Justice (Department) submitted a proposal to Congress, to amend Title 31 of the United States Code. The Department's proposal suggested that the act of bulk cash smuggling should be made a criminal offense, and that the United States should be empowered to seize and forfeit smuggled currency in accordance with the forfeiture provisions of Title 18 of the United States Code. The Congressional Record clearly states the legislative intent behind what would eventually become the Bulk Cash Smuggling Act of 2001, 31 U.S.C. § 5332.

> Confiscation of the smuggled currency is, of course, the most effective weapon that can be employed against these smugglers. Accordingly, in response to the *Bajakajian*

> decision, the Department of Justice proposed making the act of bulk cash smuggling itself a criminal offense, and to authorize the imposition of the full range of civil and criminal sanctions when the offense is discovered. Because the act of concealing currency for the purpose of smuggling it out of the United States is inherently more serious than simply failing to file a Customs report, strong and meaningful sanctions, such as confiscation of the smuggled currency, are likely to withstand Eighth Amendment challenges to the new statute.

144 Cong. Reg. H9478 (1998).

Citation to the legislative history describing the intent of 31 U.S.C. § 5332 may be useful in explaining to a court why *Bajakajian* should no longer be the applicable standard in determining the proportionality of the forfeiture in bulk cash smuggling cases.

III. Elements of the criminal offense

The following four items must be proved beyond a reasonable doubt, to establish a criminal violation of 31 U.S.C. § 5332.

- Intent to evade a § 5316 currency reporting requirement.
- Knowing concealment of more than $10,000 (in currency or other monetary instruments).
- On a person, or in a conveyance, luggage or container.
- Transport or transfer (or attempt to transport or transfer) from inside U.S. to outside U.S.

See Figure 1, page 47.

The first hurdle is to prove that the defendant intended to evade the currency reporting requirement. Here, the prosecutor's knowledge of the type, extent, and nature of the defendant's contact with the border patrol officer or agent at the port of exit becomes crucial. Was the defendant made aware of the § 5316 reporting requirement? Was the defendant a frequent international traveler? Had the defendant completed Currency and Monetary Instrument Reports (CMIRs) on previous travels? Was the defendant offered the opportunity to complete (or to amend) his or her CMIR? What was the defendant's ability to speak, read, and understand spoken or written English? Was the CMIR offered in an alternative language? If the prosecutor cannot establish this threshold element of intent to evade the currency reporting requirement, the criminal prosecution under § 5332 will fail.

The second element, that of "knowing concealment," may be an easier picture to paint for the judge or jury. The familiar proverb—"a picture is worth a thousand words"—rings true in bulk cash smuggling. The prosecutor who is fortunate enough to work with law enforcement officers who have the foresight to take photographs of the concealed currency, at the time of the encounter with the traveler or his luggage, vehicle, or package, is blessed with an easier task of proving the knowing concealment of the currency. Cash, even large sums, which are merely carried in a coat pocket, a wallet or purse, or even packed in luggage, without evidence of some effort to conceal it within the lining of the suitcase, trap, compartment, or hidden pocket, will generally not be sufficient to demonstrate that the defendant "knowingly concealed" the currency.

Proving that the crime involved "currency or monetary instruments" requires familiarity with the applicable definition of "monetary instruments." With respect to bulk cash smuggling offenses, the Code of Federal Regulations, at 31 C.F.R. § 103.11(u)(1)(i)-(v), defines "monetary instruments" as follows.

- Currency.
- Traveler's checks in any form.
- All negotiable instruments (including personal checks, business checks, official bank checks, cashier's checks, third-party checks, promissory notes (as that term is defined in the Uniform Commercial Code), and money orders)) that are either in bearer form, endorsed without restriction, made out to a fictitious payee (for the purposes of § 103.23), or otherwise in such form that title thereto passes upon delivery.
- Incomplete instruments (including personal checks, business checks, official bank checks, cashier's checks, third-party checks, promissory notes (as that term is defined in the Uniform Commercial Code), and money orders)) signed but with the payee's name omitted.
- Securities or stock, in bearer form or otherwise, in such form that title thereto passes upon delivery.

"Monetary instruments do not include warehouse receipts or bills of lading." 31 C.F.R. § 103.11(u)(2).

One emerging problem in bulk cash smuggling, from a law enforcement perspective, is the "stored value card." Currently, the definition of "monetary instruments," for purposes of prosecuting bulk cash smugglers or forfeiting seized assets pursuant to § 5332, does not include the stored value cards. According to the Federal Reserve Bank of New York:

> There are two main categories of stored value cards in the marketplace. The first prepaid cards made available to the marketplace were single-purpose or "closed-loop" cards. Gift cards, which can only be used to purchase goods at particular retailers, and prepaid telephone cards, which can only be used to make telephone calls, are examples of single-purpose cards. The second type of card to emerge was a multipurpose or "open-loop" card, which can be used to make debit transactions at a wide variety of retail locations, as well as for other purposes, such as receiving direct deposits and withdrawing cash from ATMs. Some multi-purpose cards are branded by Visa or MasterCard and can be used wherever those brands are accepted.

Federal Reserve Bank of New York, *Stored Value Cards: An Alternative for the Unbanked?* (July 2004), *available at* http://www.ny.frb.org/regional/stored_value_cards.html.

Border agents and officers do not yet have a consistent capability to check the available balances of stored value cards, to determine whether the card's available value exceeds the $10,000 threshold element set forth in 31 U.S.C. § 5332. Even if federal law enforcement agents had the ability to check the balances of these cards, the "open-loop" typed cards do not fall within the definition of monetary instruments for bulk cash smuggling prosecutorial or forfeiture purposes.

Another noteworthy facet of the Bulk Cash Smuggling Act is the requirement that the United States prove the transportation or transfer, or attempted transportation or transfer, of the currency or monetary instruments from a point inside the United States to a point outside the United States, or from a point outside the United States to a point inside the United States. The transportation or transfer element assumes that a border has been crossed. The "attempt" language, however, permits the government to charge § 5332 where the investigation is able to establish a border crossing was intended and/or was imminent. This unique language of § 5332 allows prosecutors to charge bulk cash smuggling and/or to bring civil forfeiture actions against currency or monetary instruments seized during "pipeline" stops. In *U.S.* v *One 1988 Chevrolet Cheyenne Half-Ton Pickup Truck*, 357 F. Supp. 2d 1321 (S.D. Ala. 2005), the government successfully filed a civil forfeiture action against $313,030 in U.S. currency, and against the pick-up truck which was fitted with two traps that contained the $313,030 in currency. The district court held that the volume of money hidden in the truck, along with a canine alert and the manner of packaging, was probative of illegal drug activity. However, with respect to forfeiture under 31 U.S.C. § 5332, the court stated:

> The argument in favor of civil forfeiture under the Bulk Cash Smuggling Act may be even more compelling. If the Court understands Aguila's position properly, he contends that he brought the truck, laden with several hundred thousand dollars in concealed U.S. currency in small bills, across the Mexico-U.S. border more than a week prior to its seizure. There is no evidence that Aguila ever reported such a massive quantity of cash to U.S. officials before bringing it across the border, as required by the currency reporting requirements of 31 U.S.C. § 5316. Indeed, Aguila's having concealed the currency in secret compartments is compelling evidence that he "with the intent to evade a currency requirement under section 5316, knowingly conceal[ed] more than $10,000 in currency" in the truck, in violation of the Bulk Cash Smuggling Act, 31 U.S.C. § 5332(a)(1). Such a violation would in turn subject the cash and the vehicle to the civil forfeiture provisions of that Act, under § 5332(c)(1)-(3).

Id. at 1331 n.18.

The civil forfeiture action was filed in Alabama, which does not share a land border with a foreign country. Thus, even judicial districts which do not see a high volume of the traditional border nexus cases may see cash seizures develop into bulk cash smuggling cases.

IV. Asset forfeiture

Title 31 provides for both criminal and civil forfeiture of currency and monetary instruments involved in bulk cash smuggling. In fact, criminal forfeiture is fairly broad and mandates the forfeiture of any property, real or personal, involved in, or traceable to, the bulk cash smuggling offense. Many experts agree that bulk cash smuggling may now be the most common form of money laundering. Thus, it is appropriate that the forfeiture provisions of the bulk cash smuggling statutes mirror the "involved in or traceable to" language of the forfeiture provisions governing money laundering. "[T]he court, in imposing sentence [for bulk cash smuggling under 31 U.S.C. § 5332(a)(1)]..., shall order that the defendant forfeit to the United States, any property, real or personal, involved in the offense, and any property traceable to such property." 31 U.S.C. § 5332(b)(2).

Prior to December 17, 2004, the statute contained the language "subject to subsection (d)." However, subsection (d) was never enacted by Congress. Subsection (d) would have set forth the mitigating factors to be considered by the courts in determining whether the amount to be forfeited should be reduced. However, this error was corrected when Pub. L. No. 108-458, 118 Stat. 3638, Title VI, § 6203(h), December 17, 2004, amended the statute, where § 6203(h)(1) struck, "subject to subsection (d) of this section" following "property" and § 6203(h)(2) struck, "subject to subsection (d) of this section," following "may be seized and." Thus, claimants no longer may argue that the statute is "unconstitutionally vague" because of the absence of subsection (d). *See U.S. v Hansen*, No. 2:04-CR-00091, *Order Denying Defendant's Motion to Dismiss Count Two of the Indictment as to Erik Hansen* (Docket No. 65, S.D. Ohio Oct. 20, 2004).

Title 31 also provides that, "[a]ny property involved in a violation of [31 U.S.C. § 5332(a)]..., or a conspiracy to commit such violation, and any property traceable to such violation or conspiracy, may be seized and forfeited to the United States." 31 U.S.C. § 5332(c). Civil forfeiture proceedings may be brought against any property "involved in" the bulk cash smuggling offense, including:

> any currency or other monetary instrument that is concealed or intended to be concealed in violation of subsection (a) or a conspiracy to commit such violation, any article, container, or conveyance used, or intended to be used, to conceal or transport the currency or other monetary instrument, and any other property used, or intended to be used, to facilitate the offense....

31 U.S.C. § 5332(c)(3).

Prosecutors may wish to proceed with civil forfeiture proceedings parallel to any criminal prosecution, or may elect to proceed with civil forfeiture alone. The evidence, in some instances, may not be sufficient to meet the "beyond a reasonable doubt" burden of proof inherent in a criminal case. That same evidence, however, may be more than adequate to prove forfeitability of the asset by a preponderance of the evidence, in a civil case.

Assets seized in conjunction with a violation of 31 U.S.C. § 5332 may also be administratively forfeited. In general, all property subject to forfeiture may be forfeited administratively except:

- real property (*see* 18 U.S.C. § 985);
- personal property having a value > $500,000, unless it is:
  a. merchandise, the importation of which is prohibited,
  b. a vessel, vehicle or aircraft used to import, export, transport or store controlled substance, or
  c. a monetary instrument (as defined by 31 U.S.C. § 5312(a)(3) - but NOT bank accounts! (*see* 19 U.S.C. § 1607); and
- property forfeitable under a statute that does not incorporate Customs laws (*see*, *e.g.* 18 U.S.C. § 492, related to counterfeiting).

Asset Forfeiture Policy Manual (Jan. 2007) Chap. 2 Sec. I.A.

V. Sentencing

According to the United States Sentencing Commission, *Guidelines Manual* § 2S1.3 (Nov. 2006), a bulk cash smuggling conviction, in violation of 31 U.S.C. § 5332, will result in a base offense level of 6. The offense level must then be adjusted according to the amount of the currency or monetary instruments which were smuggled, utilizing the Theft and Fraud Table set forth in § 2B1.1. USSG § 2S1.3. The minimum amount that must be added to the base offense level for

bulk cash smuggling offenses is 4 levels for "more than $10,000." (Any amount less than $10,000 would not satisfy the threshold element of § 5332.) The maximum amount that may be added to the base offense level for bulk cash smuggling, from the Theft and Fraud Table in § 2B1.1, is 30 levels (for an amount more than $400 million).

After adjusting the base offense level according to the amount of the smuggled currency or monetary instruments, 2 levels should also be added if the conviction is for bulk cash smuggling. USSG § 2S1.3(b)(1). This two-level increase for bulk cash smuggling has been upheld, over the defendant's objection that the enhancement constituted "double counting." *See U.S. v. Meza-Quinones*, 2006 WL 504282 (W.D. Tex. Feb. 15, 2006).

For purposes of illustration, assume that the traveler is convicted of bulk cash smuggling in violation of 31 U.S.C. § 5332, and that he had smuggled $350,000 in cash. According to the *Guidelines Manual*, the base offense level would be 6. USSG § 2S1.3. Because the amount involved is more than $200,000 but less than $400,000, the traveler would receive a 12 level increase based on the Theft and Fraud Table. USSG §2 B1.1. Additionally, because the traveler was convicted of bulk cash smuggling, two additional levels are added pursuant to § 2S1.3(b)(1). Thus, the traveler's adjusted offense level is 6+12+2=20. If the traveler's criminal history falls within Category I (zero or one criminal history points), the recommended sentencing range under the *Guidelines Manual* is 33-41 months of imprisonment. USSG § 5A. This represents a significant increase from the sentencing guidelines antecedent to the Bulk Cash Smuggling Act where, based on an application of the November 2000 Sentencing Guidelines, smuggling $350,000 (a violation of 31 U.S.C. § 5316) would have resulted in a sentence recommendation of only 15-21 months.

VI. Mitigation

If the evidence establishes that the bulk cash smuggler was not engaged in any other criminal endeavor, it may be necessary to balance the criminal act(s) versus the amount of the seizure. The mitigation was originally addressed in the draft version of 31 U.S.C. § 5332 as subsection (d). However, since the statute is now silent as to the mitigating factors, the courts must consider whether mitigation is appropriate on a case-by-case basis. To seek mitigation, the smuggler has the burden of proving that the currency was from a legitimate source, and was not intended for any unlawful purpose.

Tax evasion is one such "unlawful purpose" that a court may find weighs against mitigation of the forfeiture. Courts may justify full forfeiture of currency or monetary instruments in "clean money" cases. Many outbound CMIR and bulk cash smuggling violations may involve situations where the funds were earned legally, but the smuggler wanted to evade tax consequences. Thus, although the funds may be from a legitimate source, if they are intended for an unlawful purpose—tax evasion—the claimant should not be entitled to mitigation of the forfeiture.

In *U.S. v. Six Negotiable Checks in Various Denominations Totaling One Hundred Ninety-One Thousand Six Hundred Seventy-One Dollars and Sixty-Nine Cents*, 389 F. Supp. 2d 813, (E.D. Mich. 2005), a traveler was about to embark on a flight outbound from Detroit to Tel Aviv. The traveler declared that he was carrying $9,000, but he actually had $8,500 in currency, and thirteen checks (six of which were negotiable) totaling $250,671.69. The government argued that the traveler's purpose for the CMIR violation was tax evasion. The court held both that forfeiture was proper and that forfeiture of the full amount of the seized monies was not excessive. The court based its decision on the following rationale: (1) tax evasion is not a lawful purpose; (2) fines for tax evasion, willful failure to file a tax return, and CMIR violations ranged from $25,000-$250,000; and (3) while the amount of forfeiture was somewhat greater than the $250,000 maximum fine, it was not so much greater that it constituted a "gross disproportionality." *Id.* at 826.

VII. Law enforcement: why do we need § 5332?

The effective enforcement of the Bank Secrecy Act forces drug dealers, and other criminals engaged in cash-based businesses, to avoid use of domestic banks and legitimate money transmitting businesses. A drug dealer who wires millions to his account in some island banking destination creates the risk of a financial institution generating a Currency Transaction Report, or a Suspicious Activity Report. Thus, in order to avoid banks, the criminals are forced to move large quantities of currency in bulk from, to,

and through, airports, border crossings, and ports of entry, in order to eventually deposit their ill-gotten gains into foreign bank accounts.

While narcotics trafficking accounts for a substantial portion of currency smuggling, not all bulk cash smuggling involves narcotics proceeds. Alien smuggling and the smuggling of firearms and weapons are two of the fastest growing criminal enterprises, in terms of the amount of cash proceeds generated by the crime. Human trafficking is largely a cash-based business where the cash generated in the United States finds its way back to the country from whence the victims are kidnaped or indentured. Bulk cash smuggling is also an easy way to funnel monies in material support of terrorism. Border cash seizures may also represent the proceeds from the sale of imported counterfeit merchandise, or may even be monies wrongdoers are carrying across the border for the purpose of bribing foreign officials, and ultimately continuing to smuggle illegal imports or exports.

The transportation and smuggling of cash across our borders may now be the most common form of money laundering. Even the courts have recognized that, in the end, legitimate businesses simply do not smuggle loads of currency across the border to bring their transactions to fruition.

> A common sense reality of everyday life is that legitimate businesses do not transport large quantities of cash rubber-banded into bundles and stuffed into packages in a backpack. They don't, because there are better, safer means of transporting cash if one is not trying to hide it from the authorities....

U.S. v. $242,484, 389 F.3d 1149, 1161 (11th Cir. 2004).

In sum, the Bulk Cash Smuggling Act, 31 U.S.C. § 5332, despite its relative youth, is an effective law enforcement tool that assists the efforts of the United States to stem the flow of unreported cash into and out of the country. Interestingly, the necessity for the statute may, in some ways, be attributed to law enforcement itself. Strict implementation and monitoring of financial institutions' compliance with the Bank Secrecy Act effectively shifted the movement of criminal proceeds out of the channels of mainstream commerce, and into the underground bulk cash movement. It is an exciting period as new developments in case law continue to emerge and shape the practice of both prosecutors and those on the front line of our borders.

VIII. Acknowledgment

Much of what the author has learned of bulk cash smuggling is directly attributable to the expertise of Stefan D. Cassella, *Bulk Cash Smuggling and the Globalization of Crime: Overcoming Constitutional Challenges to Forfeiture under 31 U.S.C. § 5332*, 22 BERKELEY J. INT'L L. 98 (2004). Mr. Cassella is the Deputy Chief of the Legal Policy Unit, Asset Forfeiture and Money Laundering Section, Criminal Division, United States Department of Justice.❖

ABOUT THE AUTHOR

❑**Rita Elizabeth Foley** is an Assistant United States Attorney in the Asset Forfeiture Unit of the U.S. Attorney's Office in Detroit. Before joining the U.S. Attorney's Office in 2002, she served as Associate Counsel for the State of Michigan Attorney Discipline Board.✠

The viewpoints expressed in this article are those of the author and do not in any way represent the official position of the United States Department of Justice.

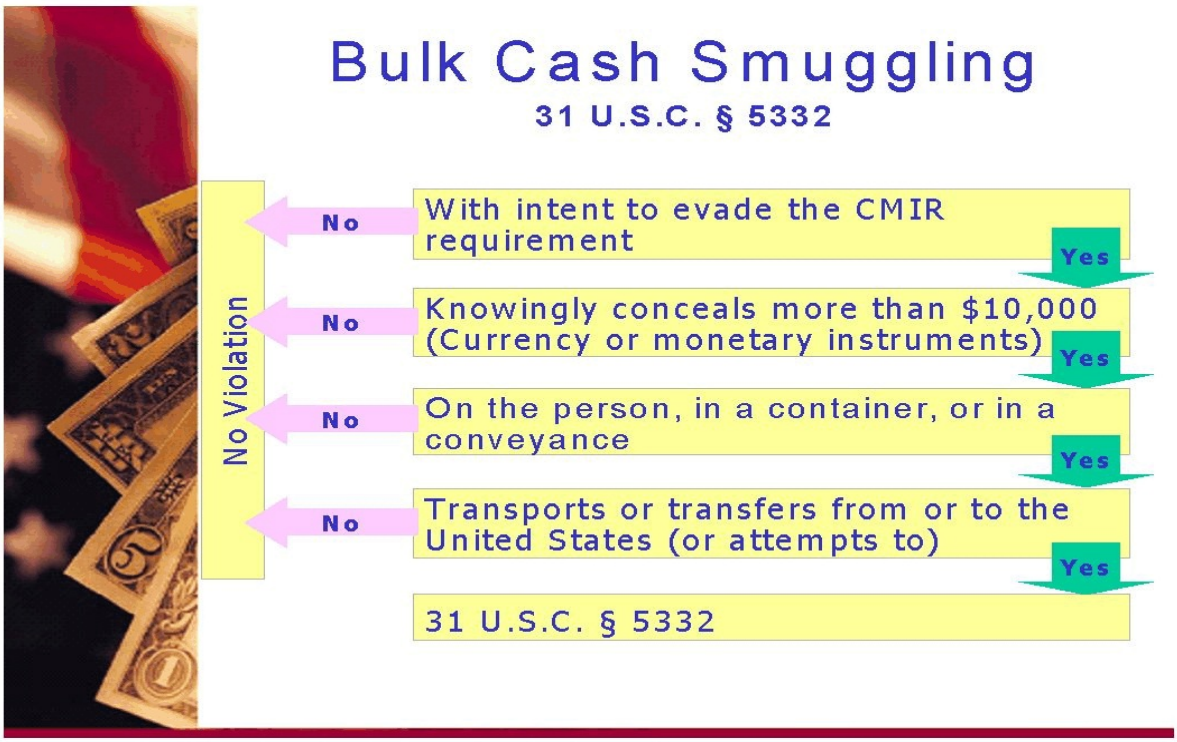
Bulk Cash Smuggling
31 U.S.C. § 5332
No Violation
No
With intent to evade the CMIR requirement
Yes
No
Knowingly conceals more than $10,000 (Currency or monetary instruments)
Yes
No
On the person, in a container, or in a conveyance
Yes
No
Transports or transfers from or to the United States (or attempts to)
Yes
31 U.S.C. § 5332

Figure 1

Sources of Information in a Financial Investigation

Alan Hampton
Special Agent
Internal Revenue Service
Criminal Investigation

I. Introduction

Financial investigations are critical to almost every investigation undertaken by federal law enforcement agencies. The profits which drive the criminal organization, and the financial tools which criminals use to protect those profits, are the main points of vulnerability. Money motivates the crime; money keeps the organization going; protecting the money is the criminal's chief concern. A financial investigation follows the money in order to take down the criminal, as well as the whole enterprise that supports the criminal activity. In focusing on the economic organization and motivation of the criminal enterprises, financial investigations emerge as a powerful tool in the law enforcement arsenal.

The author, while working in the New Orleans and Dallas field offices for the past fifteen years, has investigated cases involving legitimate enterprises from commercial fishermen to politicians and illegal ones from alien smuggling to terrorism. Developing the financial side of cases involves knowing where to look for large transactions involving the movement of money and acquisition of assets. Once the information is gathered, it needs to be presented in a format understandable to the audience. A threshold challenge is mastering the financial investigative tools available to most federal law enforcement agencies, and learning how to extract information from them.

The past few years have seen an explosion of information available to law enforcement. The following case example is illustrative of the information needed to investigate the case, and the steps required to get that information in usable form for prosecution.

II. Case scenario

Gunvant Shah operated an unlicensed money transmitting business, primarily in New Jersey and Boston. He had a network of coconspirators who funneled money through the bank accounts of legitimate companies, into foreign countries, by the use of a hawala system, thereby evading any country's reporting requirements. *See,* David Marshall Nissman, *Hawala,* UNITED STATES ATTORNEYS' BULLETIN, May 2002, at 13. This network allowed Shah to transfer illegal alien smuggling fees from the United States back to the alien smugglers in India and around the world. Shah eventually cooperated and was sentenced for his role in the scheme. *United States v. Singh*, No. 3:98-cr-00363-3 (N.D. Tex. July 22, 1999).

A. First steps

The subject(s) must be identified, the source of the money must be ascertained, and the person to whom the money is being sent must be located, in order to obtain convictions and make full use of asset forfeiture. Physical surveillance in the *Shah* case showed the subject mailing envelope-sized packages nearly every day, and trash runs garnered phone records, bank statements, and utility bills, among other things. From that information, the subject was confirmed.

After identifying the subject, requests for financial information were sent to the Financial Crimes Enforcement Network (FinCEN) and Internal Revenue Service (IRS) lead development centers (LDC) to find any financial trends that would shed light on Shah's activities. The FBI has a unit in Savannah, Georgia, that provides the same information as the IRS LDC, less tax return information. Most federal agencies have a liaison to FinCEN through whom FinCEN requests can be sent.

At the same time these investigative avenues were pursued, a mail cover was placed on the subject's residence. It showed an inordinate amount of incoming mail from an unusually high number of individuals. Mail covers are obtained by organizational requests to the U.S. Postal Inspection Service. Mail covers record the addressee and addressor of incoming mail to a designated address for a specified period of time.

Grand jury subpoenas were issued to banks, phone companies, and mail delivery services, such

as Federal Express (FedEx) and United Parcel Service (UPS). It is important to get account opening documents when subpoenaing bank records, including the signature card and the initial application. They can be used to show ownership or control of the account, and link a subject to other associated individuals.

Review of the data and information revealed that the subject did not use traditional banking methods exclusively. Search warrants for packages that the subject mailed were obtained and revealed that checks, money orders, and cash, was being sent to various destinations around the world. The details of the investigation were relayed to FinCEN analysts, and they suggested that the subject might be using an underground money transfer system. Contact was made with a FinCEN underground banking expert, and he confirmed that the subject appeared to be using the hawala system of money transfer.

"Hawala" is a term that describes an alternative banking system that operates outside of, or parallel to, "traditional" banking or financial channels. The hawala transfer system emerged in India and Southeast Asia, and predates the introduction of western banking practices. The individuals conducting the hawala transactions are called hawaladars. It is currently a major remittance system used around the world. It is but one of several such systems; another well-known example is the "chop," "chit," or "flying money" system indigenous to China. Although these systems are often referred to as "underground banking," they often operate in the open with complete legitimacy, and are often heavily and effectively advertised.

In 1999 (effective in 2001), the Secretary of the Treasury promulgated regulatory definitions of certain nonbank financial institutions for purposes of the Bank Secrecy Act (BSA), and grouped the definitions into a separate category of financial institutions called "money services businesses" (MSBs). These businesses must license with the state in which they do business (if the state has a licensing requirement) and must register with FinCEN, unless an exception to the registration requirement applies. Forms for registration are available on the FinCEN Web site at www.fincen.gov. Failure to license and register the business may result in prosecution under Title 18 U.S.C. § 1960, which makes it an offense to conduct an unlicensed money transmitting business. Importantly, proof that the funds involved in the business derived from crime (or were intended to promote crime) is not required to obtain a § 1960 conviction. Numerous cases have been prosecuted under § 1960 in recent years.

B. FinCEN

FinCEN also administers the BSA, our nation's first and most comprehensive anti-money laundering statute. The BSA requires depository institutions, other financial institutions, and trades vulnerable to money laundering, to take a number of precautions against financial crime. These precautions include filing and reporting certain data about financial transactions possibly indicative of money laundering, such as cash transactions over $10,000 and suspicious transactions. Over 15,000,000 BSA reports are filed each year by thousands of U.S. financial institutions, providing a wealth of potentially useful information to agencies whose mission it is to detect and prevent money laundering, other financial crimes, and terrorism.

Accordingly, FinCEN makes available to appropriate federal, state, and local law enforcement, and regulatory agencies, the following databases.

- **Currency and Banking Retrieval System (CBRS)**: This financial database consists of reports that are required to be filed under the BSA, such as data on large currency transactions conducted at financial institutions or casinos, suspicious transactions, and international movements of currency or negotiable monetary instruments. This information often provides invaluable assistance for investigators because it is not readily available from any other source and it preserves a financial paper trail for investigators to track criminals' proceeds and their assets. In general, CBRS data includes:
    - Suspicious Activity Reports (SARs) (filed by Depository Institutions, Casinos, MSBs, Securities & Futures Industries, Insurance Businesses).
    - Currency and Monetary Instruments Reports (CMIRs).
    - Currency Transaction Reports (CTRs).
    - Casino CTRs.
    - Reports of Over $10,000 Received in a Trade or Business (Form 8300).

- Registration of Money Services Business (RMSB).
- Foreign Bank Account Reports (FBARs).

- **Commercial Databases**: Information from commercially available sources plays an increasingly vital role in criminal investigations. Commercial databases include information such as state corporations, property, and people locator records, as well as professional licenses, and vehicle registrations.
- **Law Enforcement Databases**: FinCEN is able to access various law enforcement databases through written agreements with each agency. FinCEN requests could also include a USA PATRIOT Act § 314(a) information request. A Section 314(a) form is a request to FinCEN from a federal law enforcement agent, and can be used in a terrorism or major money laundering related investigation. Once FinCEN receives the request, FinCEN sends a notice for information to financial institutions across the country via a secure Internet Web site. The request contains subject and business names, addresses, and as much identifying data as possible, to assist the financial industry in searching their records. The financial institutions must query their records for data matches, including accounts maintained by the named subjects during the preceding twelve months and transactions conducted with the subjects within the last six months. Financial institutions have two weeks from the transmission date of the request to respond to the § 314(a) information request. If the search uncovers any matching accounts or transactions, the bank notifies FinCEN. FinCEN prepares a report of "hits" and replies to the agent within two weeks. The agent determines whether or not to subpoena the aforementioned records.

C. Next steps

A Title III wire telephone interception (phone tap) was used during the Shah investigation, which allowed the government to intercept telephone calls in which Shah and coconspirators discussed their plans. The phone tap also allowed the government to intercept faxed items, which included ledger sheets detailing the balances for each of the hawaladars.

Shah collected currency and monetary instruments used to pay for alien smuggling, including cash, cashier's checks, money orders, and personal checks, in New Jersey and Boston, and typically sent money to India in three different ways. The first system was a true direct hawala transfer with hawaladars in India. Shah called his connections in India and they transferred the money to its destination. In return, Shah sent money around the United States on behalf of the hawaladars in India.

The second system was the transfer of monetary instruments by FedEx to another hawaladar who operated a Canadian company in Toronto, Canada. The Canadian company then wired money to companies through its network of other hawaladars and eventually to India.

The third system utilized an international metal brokerage company in New York with its own network of money movement around the world. Since all three avenues involved the transfer of proceeds of a specified unlawful activity (SUA), as defined in 18 U.S.C. § 1956(c)(7), all three avenues involved possible money laundering violations, and the funds involved in those transactions were, therefore, subject to civil forfeiture under 18 U.S.C. § 981(a)(1)(A) & (C) and 28 U.S.C. § 2461(c).

III. Asset forfeiture

Title 18 U.S.C. § 981 allows for the civil seizure and forfeiture of assets relating to 18 U.S.C. §§ 1956, 1957 (money laundering), 1960 (unlicensed money transmitting business), foreign crimes, proceeds from other criminal violations including offenses constituting an SUA, automobile theft and car jacking, and assets of a domestic or international terrorist. Section 982 is the analog to § 981 that is used for criminal forfeiture. In the case of some BSA violations, (structuring and Currency and Monetary Instrument Report (CMIR) violations)), 31 U.S.C. § 5317 provides for civil and criminal forfeiture.

Title 18 U.S.C. § 984 provides a statutory exception to the usual rule regarding strict tracing that would otherwise apply in civil forfeiture cases brought under 18 U.S.C. § 981(a)(1)(A) or 31 U.S.C. § 5317(c)(2). Title 18 U.S.C. § 984 applies in any civil forfeiture action in which the subject property is cash, monetary instruments in bearer form, funds deposited in an account in a financial institution, or precious metals. Any identical property found in the same place or

account as the property involved in the offense that is the basis for the forfeiture is subject to forfeiture under 18 U.S.C. § 984.

For example, suppose a person placed $10,000 in laundered funds in a bank account on Monday and the account is seized for civil forfeiture on Friday. Suppose also that, at the time of the seizure, the balance in the account is $10,000, but that in between these dates, on Wednesday, the balance dropped to zero and subsequently $10,000 in unlaundered funds are deposited. Consequently, the $10,000 in funds that remain on Friday cannot be strictly traced back to the money laundering offense. In general, the $10,000 seized on Friday is not the same money as the laundered funds that were placed in the account on Monday. Under a traditional tracing analysis, the government would not be able to forfeit the $10,000. Under 18 U.S.C. § 984, however, the government may forfeit the $10,000 from the account, without regard to fluctuations in the balance in the account. Any action that utilizes § 984 to forfeit property, not traceable directly to the offense that is the basis for the forfeiture, must be commenced not more than one year from the date of the offense.

IV. Information from foreign countries

Some of the information needed in the example case scenario was in foreign countries. The investigating agent had to determine the best way to get usable information from them. Contact with the agencies' attachés (IRS, FBI, ICE) can sometimes yield quick, but nonevidentiary, information. The Office of International Affairs (OIA) in the Criminal Division of the Department of Justice (Department) can advise regarding the various foreign treaties and requests available with foreign countries. The United States also has tax treaties with certain countries.

Records requested through a tax treaty can only be used for tax administration purposes, and not other criminal charges. If a grand jury tax investigation includes the investigation of money laundering and other Title 18 charges, the records obtained through the tax treaty are useable to support the tax charges, but the jury would have to be advised to ignore this evidence when considering the other nontax charges. To avoid this dilemma, consider using a different legal method to obtain the records, such as Mutual Legal Assistance Treaties (MLATs).

Generally speaking, there are two nontreaty methods for obtaining foreign bank records. First, the *Bank of Nova Scotia* subpoena can be used to subpoena records, in overseas branches, from banks that have branches in the United States. For example, if the subject has an account with HSBC in Hong Kong, the branch in the United States may be served. However, prior to issuing such a subpoena, a prosecutor must first obtain OIA approval pursuant to guidelines set forth in the Criminal Resource Manual. *See United States Attorneys' Manual* § 9-13.525.

A second method to obtain foreign bank records involves the use of 31 U.S.C. § 5318(k), a provision added in the USA PATRIOT Act. Section 5318(k) allows law enforcement agents to get bank records from a foreign bank that has a correspondent bank account in the United States. Almost all the banks in the world have a relationship with a bank in the United States, therefore, most bank records are theoretically within reach. The way it works is that the § 5318(k) subpoena is served on the correspondent bank in the United States. The foreign bank is then required to supply the records or the U.S. correspondent bank may face fines of up to $10,000 per day or until they terminate their correspondent banking relationship. These subpoenas are administrative and can only be issued by the Secretary of the Treasury, the Assistant Attorney General of the Criminal Division, or the U.S. Attorney. Before any § 5318(k) subpoena can be issued, it must first be approved by the Director of the OIA, who will consult with the Chief of the Asset Forfeiture and Money Laundering Section (AFMLS), as well as the Treasury and State Departments. Approval for such subpoenas has been granted only in a handful of cases because the preferred method of obtaining information concerning foreign bank accounts is through the MLAT process.

FinCEN is also a member of the Egmont Group, an international organization of Financial Investigative Units (FIU). FinCEN, for example, is the FIU for the United States. The Egmont group maintains a Web site at www.egmontgroup.org. The goal of the group is to create a global network by fostering cooperation between countries by sharing information. Requests can be made through FinCEN for additional information. Information obtained through the FIU process is lead information only and cannot be used as evidence in judicial proceedings.

In the Shah investigation, an MLAT request with Canada yielded bank records and an interview with the Canadian hawaladar. Since money laundering and informal banking in Canada is legal and he did not know the source of the funds, the witness answered all questions and laid out the entire path of his financial network.

V. Internal Revenue Service Lead Development Centers

Another excellent source of information is the IRS *Reveal* system. The *Reveal* system provides IRS criminal investigation (CI) agents and analysts with the capacity to access, analyze, and interpret data from a spectrum of sources uploaded in a single stand-alone system. *Reveal* provides users with the capability to search multiple data sources at one time on a single set of criteria. Those data sources are public record databases, as well as the financial data contained in the CBRS. *Reveal* can provide data visualization by linking identifying factors such as subjects, accounts, and identification numbers, and provides clear representation of networks.

The *Reveal* system is used by investigative analysts at CI's LDCs and within the SAR Review Teams in each CI field office. Access to this information must be requested through an IRS Special Agent since there are tax return disclosure aspects. If an IRS agent is assigned to the case and tax charges are being pursued, a grand jury expansion to include tax charges should be sought.

If tax charges are not included in the prosecution, the tax return information gained from the investigation may not be usable in court proceedings. An alternate method of getting and using tax return information is by ex parte application and order. These requests are signed by a District Judge and forwarded to the IRS Disclosure Office for processing. Tax returns are useful in almost every financial investigation, and can be used to see if the subject is reporting the income from an illegal activity or if the subject is using a legitimate business to launder illegally-derived funds. If there are no plans to pursue tax charges, it is strongly advisable to acquire any related tax returns through the ex parte process.

In the example investigation, results from FinCEN showed numerous cash transactions, as well as postal money order purchases. The cashed portion of the money orders were obtained, which revealed where and how they had been redeemed. The money orders had been deposited into a bank account of an international metals broker with offices in New York. Subpoenas were issued for that account, which showed enormous amounts of cash and cash equivalent being deposited, and corresponding wires being sent all over the world. Since the payments for alien smuggling fees from Shah were proceeds of an SUA, they were subject to forfeiture. The civil statute, 18 U.S.C. § 981, was used to forfeit those proceeds.

Bank records were subpoenaed and all relevant databases checked. The only place left with unknown information was the subject's residence. It is much easier to get a search warrant for a business than a residence, but articulation for a financial search warrant of a residence is also relatively easy. Since financial documents are generally stored for a long period of time, probable cause can usually be maintained for up to six months, as long as all circumstances remained the same. *See. e.g., United States v. Hanton*, 2006 WL 1920358 (4th Cir. July 12, 2006) (unpublished) (search warrant for documents relating to money laundering upheld even though events identified in the affidavit occurred three years before the search warrant was issued). The other advantage of a financial search warrant is that it allows access to, and permission to search, all areas of the property.

The information gathered was used to obtain the search warrant of the residence. The FinCEN hawala expert informed the investigative team that safe deposit boxes are commonly used by hawaladars to store gold and jewelry, which is sometimes used for payment instead of cash. Warrants were executed and hawala ledgers detailing all of the subject's transactions, cash, and cash equivalents, were found.

VI. Selecting the charges against Shah

The prosecutor knew that he planned to indict Shah for alien smuggling, but were there other charges to consider? Aliens were smuggled from India to the United States and payments were made to the smugglers. A majority of the payments were made in the United States to Shah. Shah then transferred the money from the United States to India. Primarily, Shah was an illegal money transmitter, in violation of 18 U.S.C. § 1960.

He was not licensed by the state or registered with FinCEN and yet he transmitted money, or

acted as a bank. Shah knew the money he received was "black" money, or proceeds of an SUA. Had he participated in a transaction that affected interstate commerce with more than $10,000 of that money, he could have been charged with money laundering in violation of 18 U.S.C. § 1957. However, Shah usually dealt in smaller amounts and did not "spend" any of the money, so he did not violate this statute.

It could be argued that Shah, by sending money through his network, promoted the scheme, or disguised the source and nature of the proceeds. Shah had money in the United States (could have been clean money) and sent money outside the United States to promote the SUA, in this case alien smuggling, which is a violation of 18 U.S.C. § 1956 (a)(2)(A). This statute is the only money laundering statute that does not require the proceeds of an SUA to have a money laundering transaction.

Shah's purchase of postal money orders was designed to stay under the $3,000 record keeping requirement outlined in 31 U.S.C. § 5325. He was also guilty of structuring to avoid the $3,000 threshold, a violation of 31 U.S.C. § 5324(a). The reports generated by FinCEN or by the IRS *Reveal* system showed, in spreadsheet format, the postal money orders purchased by time and date. The spreadsheet would also show other transactions, such as deposits of cash to avoid the $10,000 reporting requirement, or transactions of $10,000 or more by financial institutions, wire remitters, or businesses. Violations of both statutes could lead to civil or criminal forfeiture.

VII. Other sources of information

The more information the prosecutor has, the easier it is to make a decision on how to charge a case. Additional sources of information are listed below, and there are obviously numerous other sources. Access to information will continue to expand with more powerful tools, but they are no good unless the team knows where to find them and how to use them.

- SAR Review Teams are typically comprised of agents from IRS, DEA, ICE, FBI, and various other federal, state, and local law enforcement agencies. There are approximately eighty SAR Review Teams throughout the United States. The teams review all suspicious activity reports submitted by the various financial entities including banks, MSBs, casinos, and others within their respective geographical areas. The teams look for patterns and possible violations for further investigation.

  Instances where a SAR has merited further investigation include those where an individual or business deposited a significant amount of cash in structured transactions. In the case of businesses handling large sums of cash, for example a car dealership, SAR Review Teams also examine the transactions to determine if the business filed Forms 8300 on the large cash transactions. Businesses are required to file Forms 8300 if they receive more than $10,000 in cash in a single transaction or related transactions from an individual sale or customer. Car and boat dealers are the most likely candidates for this type of requirement. Individuals with large amounts of cash tend to buy boats and cars, but know the sellers have to file the Forms 8300, so the buyers or sellers attempt to find ways around the reporting requirement. The IRS has successfully prosecuted entities subject to Form 8300 requirements using undercover techniques. During these investigations, undercover agents attempt to buy items with purported proceeds of an SUA to see if the dealer attempts to avoid reporting requirements. If the dealers knowingly take proceeds of an SUA or "sting" money, the "sting" money, the luxury item purchased, and possibly the entire business, is subject to forfeiture.
- The Fedwire system is a system owned and operated by the Reserve Banks that enables financial institutions to electronically transfer funds between its approximately 9,000 participants. The database contains information for the vast majority of wire transfers over the last five years, in which at least one party is a U.S. bank customer. These records can be accessed through the Federal Reserve Board.
- Investigative Data Warehouse (IDW) is an FBI research tool that can access information from a variety of sources, including FBI Forms 302, bank and telephone records that have been subpoenaed from other cases around the country, and related analytical products.
- The Dun and Bradstreet Internet site at www.dnb.com, contains more than 77,000,000 global business entities.

Information available includes business names, addresses, phone and fax numbers, employee information, trade and assumed names, indictments, fraud charges, other legal events, officers and directors and their backgrounds, bankruptcies, suits, liens and judgments, financial information, and corporate affiliations and linkages to other companies.

VIII. Terrorism cases

Terrorism cases allow for the use of all of the above mentioned techniques, including the FinCEN 314(a) requests, which are used to access financial institutions for accounts held in the name of subjects of interest in money laundering and terrorism investigations. Other sources of information include the following.

- Airline Reporting Corporation (ARC) has records on approximately half of all airline ticketing done in the United States. These records contain domestic flight and credit information for airline ticket purchases from U.S. travel agencies.
- The National Counterterrorism Center (NCTC Online) is the central and shared knowledge bank on terrorism information, and provides source intelligence support to government-wide counterterrorism activities by the FBI, CIA, Departments of State, Defense, Energy, Health and Human Services, Homeland Security, Nuclear Regulatory Commission, and the U.S. Capitol Hill Police.
- The FBI's Terrorism Financing Operations Section (TFOS) can request the CIA to search for various items, but the information has to suggest a "nexus to terrorism." Information need not be conclusive, but should have either source information or relationships with other international terrorism subjects. This information is usually for intelligence purposes only, and not for legal proceedings.

IX. Conclusion

As the discussion above indicates, there are numerous sources of financial information available to investigators. If you need further information about any of these sources or have any questions, contact your local IRS agent or the Department's AFMLS at (202) 514-1263.

***Note*:** The Organized Crime and Drug Enforcement Task Force and AFMLS conduct several intensive one-week Financial Investigation seminars around the country each year for investigators and prosecutors. For information about these seminars, contact AFMLS.❖

ABOUT THE AUTHOR

❑**Alan Hampton** has been a Special Agent with IRS Criminal Investigation since 1991 and has worked in the New Orleans and Dallas field offices. He has been assigned to the Joint Terrorism Task Force in Dallas since 2001. He has been a member of the IRS Money Laundering Expert Witness Cadre since 2004.✠

Criminal Prosecution of Banks Under the Bank Secrecy Act

Lester Joseph
Principal Deputy Chief
Asset Forfeiture and Money Laundering Section
Criminal Division

John Roth
Chief of the Fraud and Public Corruption Section
U.S. Attorney's Office
District of Columbia

I. Introduction

Since it was enacted in 1970, the Bank Secrecy Act (BSA) has provided for civil and criminal penalties against individuals or banks that violate its provisions. Prior to 1996, the primary BSA requirement for financial

institutions was to file Currency Transaction Reports (CTRs). There have been a handful of prosecutions of financial institutions over the years for the failure to properly file CTRs. Since that time, however, several new statutory and regulatory requirements were enacted that imposed new antimoney laundering (AML) compliance responsibilities on banks. In 1996, Treasury Department regulations required banks to file Suspicious Activity Reports (SARs). *See* 31 C.F.R. § 103.18. In 2001, the USA PATRIOT Act required banks to establish AML programs that included the following.

- The development of internal policies, procedures, and controls.
- The designation of a compliance officer.
- An ongoing employee training program.
- An independent audit function to test programs.

31 U.S.C. § 5318(h). In short, the BSA imposes a legal obligation on banks to know their customer's business, the source of the customer's money, and the type of transactions that are typical for the customer. Banks have an obligation to report, or, in some cases, to refuse to conduct transactions they find suspicious—ones that appear to be from an illegitimate source, have no legitimate business purpose, or are out of character with what they understand their customer's business to be.

Prior to 2002, there were no criminal enforcement actions, or even serious regulatory penalties, for the failure of financial institutions to file SARs or comply with the requirements of § 5318(h). The first civil penalty against a bank for failing to file SARs was imposed on Great Eastern Bank of Miami, Florida, in September 2002. Beginning in November 2002, the Department of Justice (Department) has conducted a series of criminal investigations into financial institutions, resulting in either significant criminal convictions or deferred prosecutions of several institutions.

Some have alleged that prosecutors are criminalizing what was designed to be a purely regulatory matter, and that such actions impose criminal sanctions on what is essentially a discretionary act. While such allegations may have some appeal in the abstract, the reality is far different. A close examination of each of these cases shows compelling evidence of willful criminal conduct or a systemic failure of the institution involved to live up to its statutory obligations to have an effective AML program under the BSA. This is true for each of the cases that were brought, and there are a number of solid legal reasons why this will continue to be true in the future.

This article will discuss each of the criminal enforcement actions against banks for BSA/AML violations, the rationale for the outcome in each case, and the role criminal prosecution of banks and other financial institutions plays in compliance with the BSA and the U.S. AML program generally.

II. Broadway National Bank

In November 2002, Broadway National Bank (Broadway), in the Southern District of New York, was the first bank to be prosecuted for failing to file SARs. Broadway was used by several drug trafficking organizations to launder drug money. The bank was also used by several businesses with offices located within a few blocks of the bank branch. A minimal amount of due diligence would have disclosed that the small businesses whose accounts were used to launder the money could not have generated legitimate business in the amounts of money deposited into the accounts. After the investigation and prosecution of the drug trafficking organizations was completed, authorities turned their attention to Broadway to determine why so much laundering was going on there. Their curiosity and persistence disclosed an institution with serious compliance problems and only the shell of an AML program.

Despite being provided with numerous warnings about its legal obligations under the BSA, by both banking regulators and its own consultants, Broadway failed to establish and maintain even a minimally effective AML program. As a result, Broadway failed to report suspicious financial transactions that occurred over a two-year period, including hundreds of bulk cash deposits totaling more than $46 million, and thousands of structured deposits of more than $76 million in cash in over 100 separate accounts. Once these enormous, and highly suspicious, amounts of cash were deposited, the money was promptly wired, on the authorization of Broadway branch managers, to bank accounts located in Latin America and the Middle East, including several well known money laundering havens.

For example, from January 1996 to March 1998, a money launderer named Alfred Dauber deposited approximately $46 million in suspicious cash deposits into nine accounts at Broadway. Dauber opened the accounts claiming to be in the electronics business. In fact, during this period, Dauber participated in large-scale laundering of narcotics proceeds on behalf of a Colombian drug cartel. Typically, Dauber arranged for a runner to deliver more than $150,000 in cash—once as much as $660,645—in a single day, to a teller window for deposit into Dauber's personal bank accounts. These almost daily cash deposits were brought to Broadway in duffel bags and other containers filled with hundred of thousands of dollars in small bills, wrapped in rubber bands. After bringing a bag of cash to a bank teller, the runner typically left the bank while the cash was being counted, and picked up the emptied bag on his next visit, often the next day, when he delivered another bag containing tens of thousands of dollars for deposit.

There was so much cash brought to the bank for deposit on behalf of Dauber that the tellers often had to count all the cash during their lunch hour. They complained to senior bank officers about the time it took to count these enormous cash deposits. Often, the dollar amounts reflected on the deposit slips left in the duffel bag did not match the amount of cash in the duffel bag to be deposited into Dauber's accounts. Eventually, Dauber arranged for the tellers to complete the deposit slips. On the day of a deposit, or within a few days of a deposit, senior bank officers signed forms, at the direction of Dauber, authorizing the wiring of a significant portion of this recently-deposited cash to bank accounts in Colombia, Panama, and Miami, Florida. Broadway employees were directly involved in all the Dauber transactions, yet never made any inquiry to determine if there were business reasons for this suspicious activity. They also failed to file Criminal Referrral Forms (the predecessor to the SAR) or SARs for any of these transactions.

As a result of its criminal conduct, according to the Government's Sentencing Memorandum, Broadway became a bank of choice for narcotics money launderers and other individuals who wished to shield their financial activities from the government. Several narcotics money launderers who banked at Broadway informed the government that they chose to launder their illegal narcotics proceeds there on the recommendation of other launderers and because Broadway personnel rarely asked questions. Broadway pled guilty to a three-count Information alleging the failure to file SARs, the failure to file accurate CTRs, and the failure to have an effective AML compliance program. The guilty plea resulted in a $4 million fine. *United States v. Broadway National Bank*, No. 02 Cr.1507 (TPG) (S.D.N.Y. Nov. 27, 2002).

III. Banco Popular

Banco Popular de Puerto Rico (BPPR), one of the thirty-six largest financial institutions in the United States and the largest financial institution in Puerto Rico, was the first bank to enter into a Deferred Prosecution Agreement (DPA) for failing to file SARs, in January 2003. The bank provides complete financial services in Puerto Rico, the continental United States, and the Caribbean. As in the Broadway National Bank case, law enforcement attention focused on BPPR as a result of the investigation of several drug trafficking organizations and money laundering schemes.

First, Ferrario Pozzi used an account at BPPR to launder approximately $32 million of narcotics proceeds. Suspicious activity that went unreported by the bank included huge cash deposits (at times over $500,000 a day) that consumed hours of tellers' time to process. An investigation by the Internal Revenue Service (IRS) and the Customs Service (now Immigration and Customs Enforcement) revealed that false CTRs were filed and no SAR was filed until February 1998, *after* approximately $21 million of narcotics proceeds was laundered through the account at one branch.

The investigation revealed that the $32 million deposited into the Ferrario account consisted of cash from numerous drug trafficking organizations. Large cash deposits, made up of small denominations, numbering as many as fifteen in the course of a day, were made on a regular basis into the Ferrario account. In June 1997, the operations of the Old San Juan branch were disrupted as a result of the time it took to count Ferrario's cash. At one point, employees of the bank told Ferrario to make his deposits through the night depository to avoid tying up the teller lines. Ferrario's cash deposits required significantly more armored car pickups to transfer the money. The need for the additional trips was reported to the regional manager and the operations officer to justify the extra expense.

In October 1995, the branch manager at the Old San Juan Branch was informed by an employee that Ferrario's transactions were significant and suspicious. As early as May 1997, memoranda were sent from the Old San Juan Branch to the San Juan Regional Manager concerning the increased daily, branch cash-levels caused by Ferrario's deposits.

From June 1995 to March 1998, hundreds of wire transfers were made from the Ferrario account to over 300 locations around the world. The wire transfers occurred almost immediately after the deposits. Often, Ferrario would fax his wire instructions to BPPR from his base of operations in Colombia. Wire transfers numbered between forty to eighty a month and amounted to approximately 25 percent of the branch's daily wire activity. The wire transfers were inconsistent with Ferrario's purported business and consistent with the laundering of drug proceeds.

Between July 1995 and March 1998, BPPR filed 416 CTRs reporting Ferrario's cash transactions. Three hundred eighty four of these stated that the funds were derived from a gas station. In a single week in 1995, the same branch employee filed three CTRs listing three different sources of funds—overseas calls, a gas station, and money transfers— as the source of the cash deposits. BPPR's ability to catch this discrepancy was hampered by a lack of staffing in its money laundering compliance program.

Ferrario's business was located only two blocks from the Old San Juan Branch. Many of the branch employees walked by the business every day, and not only were they aware that the business was not a gas station, but they also rarely saw customers at the business. Tellers at the Old San Juan Branch felt that Ferrario's deposits were suspicious, and frequent comments were made among branch personnel that the money deposited by Ferrario was from illegal sources and that Ferrario was using his account to launder money. In one instance, after an argument with a teller who refused to exchange $100 bills for $20 bills, Ferarrio asked to speak to a branch manager, who then instructed the teller to find as many $100 bills as possible. Concerns about the huge volume of cash deposits and the disruption it caused at the branch were discussed at monthly branch meetings.

Despite two years of suspicious activity in the Ferrario account, the service of a subpoena on the account in August 1997, and hundreds of high-risk transactions, the bank failed to investigate Ferrario or his business until December 1997. BPPR failed to file a SAR on the Ferrario account activity until March 19, 1998, two and one-half years after the account was opened and after over $20 million of narcotics proceeds had been laundered through the account. The SAR understated the actual amount of cash deposited and the time period of the deposits, and incorrectly reported the name of the Ferrario account as "Puerto Rico Net Yellow." The reported account was an additional account maintained by Ferrario at BPPR, but it was not the account into which the cash deposits were made or from which the wire transfers were made. The SAR was virtually of no use to law enforcement. In April 1998, the Ferrario SAR was presented to the Auditing Committee of the Board of Directors of BPPR. Although this was by far the largest SAR ever presented to the Board of Directors in terms of suspected dollar amount, they took no action and asked no questions.

The second scenario involved an IRS investigation targeting Jairo de Jesus Vallejo-Jurado (Vallejo). This investigation revealed that, from late 1998 through 2000 (post-*Ferrario)*, Vallejo used two accounts at BPPR to launder nearly $2 million of narcotics proceeds by structuring cash deposits. While the bank's Large Cash Reporting System did pick up and aggregate structured transactions and file CTRs, BPPR failed to file SARs on the activity of Vallejo's accounts until November 1999, at least one year after the account activity changed dramatically. Over $1 million of narcotics proceeds had been laundered through the accounts, and three law enforcement subpoenas had been served. BPPR understated the dollar amounts for both accounts involved in the suspicious activity. Subsequent to the filing of the initial SARs, BPPR conducted its first "Know Your Customer" (KYC) visit to Vallejo. Following this visit, supplemental SARs were filed in December 1999, noting that the account activity reported on the SARs filed in November was inconsistent with the nature of Vallejo's purported business.

BPPR continued to permit Vallejo to structure deposits into 2000, even after branch managers reported that there was no justification for the deposit of cash into the accounts. Bank documentation reflects that in December 1999, BPPR contemplated closing the accounts, but decided against it. Shortly thereafter, in February

2000, the IRS asked the bank to keep the account open to facilitate the investigation of Vallejo.

Finally, from 1997 through June 2000, BPPR, through its International Banking Entity (IBE), provided banking services to foreign businesses in the Dominican Republic purportedly operating as money service businesses (MSBs). In 1997, MSBs were considered high-risk businesses for money laundering, and the Dominican Republic was considered to be a high-risk geographic area for narcotics-related money laundering.

Although BPPR knew the general purpose of the businesses in question, the bank failed to document adequately the basis for this knowledge. For example, BPPR failed to document whether any customer visits were made to these businesses prior to 1999, and the customer files relating to these accounts contained inadequate documentation as to the nature of the client's business. Although BPPR conducted KYC visits in 1999, the visitation documentation contains no information about the expected volume and type of account activity for the purported business.

From at least as early as 1997, BPPR received these businesses' checks and other items in bulk for purposes of processing, and processed the items without reviewing them. There was activity through certain of these accounts which was indicative of money laundering by the businesses or their customers, yet no SARs were filed.

In one case, BPPR failed to investigate and allowed transactions to continue even after being put on notice by law enforcement that the account might have involved criminal activity. Specifically, BPPR was served with a Drug Enforcement Administration seizure warrant relating to an account opened at BPPR that had received $275,000 from Comercial Importadora SMA, a Dominican Republic business that had also opened an account at the bank. Although the branch manager informed the account holder of Comercial Importadora that his account had to be closed, after consultation with the account holder and his lawyer, the branch manager allowed the account holder's brother to open an account on the same day the seizure warrant was received, and the account opening documentation noted that the account was a substitute for the Comercial Importadora SMA account.

In January 2003, BPPR entered into a DPA with the Department, based on its failure to detect and report money laundering activity through the bank. Per the terms of the Agreement, a one-count Information was filed charging the bank with failure to file SARs. The Information, however, would be dismissed if the bank fully complied with its obligations under the Agreement to develop and maintain an effective AML compliance program. The Information was subsequently dismissed after the one-year period. In addition, BPPR agreed to forfeit $21.6 million. Financial Crimes Enforcement Network (FinCEN) assessed a $20 million civil penalty against the bank, but this was deemed satisfied by the payment of the $21.6 million forfeiture. *United States v. Banco Popular De Puerto Rico,* No. Cr 03-317 (PG)(D.P.R. Jan. 16, 2003).

The decision to pursue a criminal prosecution of BPPR was based on the bank's repeated failures to file SARs or to take remedial action when faced with a massive and extended inflow of cash that had every earmark of being drug proceeds. The nature of these transactions became public through the prosecution of Ferrario on federal money laundering charges, after BPPR allowed this cash to flow through its bank. These events led to some efforts at reform. Shortly after the prosecution of Ferrario, BPPR still accepted the structured Vallejo deposits, and even recognized the structuring, while failing to take any timely action. Ferrario and Vallejo were convicted of money laundering, and sentenced to 97 months and 27 months, respectively. Even as the investigation of the bank proceeded, BPPR serviced the high-risk Dominican MSB accounts. However, in light of the remedial actions taken by the bank, its cooperation with the government's investigation, and its willingness to acknowledge responsibility for its actions, the government agreed to enter into a DPA instead of pursuing a criminal conviction.

IV. Delta National Bank

In October 2003, Delta Bank, a Miami-based investment bank that was owned by a Brazilian national, was the third bank to be the subject of a criminal enforcement action for the failure to file SARs. Delta Bank came to the attention of agents and prosecutors in the District of Maryland during the course of an undercover operation entitled "Operation Laundry Chute." The vast majority of the bank's customers were Brazilian or Colombian. A Colombian national, who operated an independent foreign currency exchange business in Colombia, opened three accounts at Delta Bank in 1998. The purpose of foreign

exchange businesses, such as that operated by the customer, was to act as a broker between customers who had United States dollars and wished to purchase Colombian pesos, or vice versa. Foreign currency exchange businesses in Colombia had been identified by the bank's regulator, the Office of the Comptroller of the Currency (OCC), and other federal agencies, as high-risk for money laundering the proceeds of narcotics trafficking and other criminal activity. During this period, the bank and its officers were aware of these risks, and that the customer was operating such a business.

During the period of time covered in the Information, the customer assisted other Colombian customers of the bank with transactions that were conducted as part of the foreign currency exchange business. The bank was aware of this assistance. The total amount involved in the customers' foreign currency exchange transactions was between $5 million and $10 million. The bank acknowledged that a SAR was required to be filed concerning the customer's use of the account for foreign currency exchange business, but the bank incorrectly concluded that no SAR was required, and thus willfully failed to file.

Delta Bank is an unusual case in that it involved the failure to file a SAR in transactions involving a single customer. This was not a failure of the bank's compliance program, but rather an intentional decision by the bank to allow these type transactions. Bank officers were aware of the possibility that the customer might be engaging in Black Market Peso Exchange (BMPE) transactions (a trade-based money laundering system through which South American money brokers facilitate a nonregulated currency exchange of United States dollars for local South American currency) and chose not to report the transactions as suspicious. As a result of the bank's awareness of the suspicious transactions, its failure to report them, and the fact that drug money in fact moved through the bank, the decision was made to pursue a criminal charge.

In October 2003, Delta Bank pled guilty in the District of Maryland to a one-count Information charging the bank with the failure to file a SAR on one of the transactions through the customer's account. The bank also agreed to the administrative forfeiture of $950,000. *United States v. Delta National Bank and Trust Company,* Criminal No. JFM-03-0416 (D. Md. Oct. 1, 2003).

V. AmSouth

AmSouth Bank (AmSouth) was the second institution to enter into a DPA for failing to file SARs. This was the first case involving white collar crime, rather than drug trafficking. In contrast to the previous cases, however, AmSouth attracted special scrutiny from the prosecutors because of its slow and incomplete response to grand jury subpoenas.

In the spring of 2002, the United States Attorney's Office for the Southern District of Mississippi, along with a number of federal and state agencies, began an investigation of a fraudulent promissory note scheme. The scheme was perpetrated by Louis D. Hamric, II, a licensed attorney; Victor G. Nance, a registered investment adviser employed by MONY; and various other individuals. Hamric issued the investors a promissory note assuring them of a very high interest rate for one year. Hamric had little, if any, contact with the actual investors. Various promoters of the scheme, including Nance, brought investors to Hamric and received a commission for their services. Hamric told Nance that he needed a "block" of $10 million to participate in a "trading program" that would provide returns through the promissory notes of up to 25 percent annually. Nance convinced over forty of his clients to invest in Hamric's program by making numerous misrepresentations to them about the nature and risk of the investment.

During the two year course of the "Ponzi" scheme, AmSouth officers and employees, at seven branches in four states, had contacts with Nance or Hamric that should have alerted the bank to the criminal activity. One of these employees suspected involvement in an illegal "Ponzi" scheme and reported concerns to AmSouth's Legal Department and Corporate Security. AmSouth provided a copy of each custodial account holder's bank statement to Hamric and Nance on a quarterly basis, without the knowledge or consent of the custodial account holders. Further, when the customer chose to reinvest, AmSouth agreed, without the knowledge of any of the account holders, to offset the proceeds of the old note against the new one, and send Hamric the difference.

Beginning in early 2001, several different promoters brought a second wave of investors into

the Hamric scheme. AmSouth held promissory notes assuring these new investors as much as 25 percent interest monthly. Although a note promising such interest is suspicious on its face, AmSouth did not question the terms or nature of any of these promissory notes. Hamric and Nance attracted a total of approximately $20 million in fraud proceeds, caused the proceeds to be deposited into AmSouth accounts, and transferred the proceeds among, and out of those accounts. They would not have succeeded in their schemes without AmSouth's participation.

At some point, Hamric stopped paying interest owed to the investors, and the fraudulent promissory note scheme fell apart. This triggered a number of civil lawsuits against individuals (Hamric, Nance, and others) and institutions, including AmSouth. The scheme also became the subject of several investigations by state and federal authorities, including a federal grand jury investigation in the Southern District of Mississippi.

Between April 2002 and June 2003, eight federal grand jury subpoenas were issued to AmSouth requesting the following information.

- All documents relating to the Hamric and Nance promissory note scheme, including all documents for any custodial trust accounts opened by either Hamric or Nance on behalf of an account holder.
- All documents for any bank accounts held by Hamric or Nance and various others associated with the scheme.
- All internal and external communications between any AmSouth employee and Hamric, Nance, or any custodial trust account holder.

In responding to the grand jury subpoenas, AmSouth (1) failed to timely produce certain documents called for by the subpoenas; (2) failed to produce certain documents in the manner in which they were kept in the regular course of business, as required by the subpoenas; and (3) failed to locate and produce certain documents called for by the subpoenas until AmSouth was targeted in this criminal investigation.

After being notified of concerns by AmSouth employees, AmSouth's Legal and Corporate Security Departments, in conjunction with AmSouth's management, had a legal obligation to report that Hamric might be operating an illegal scheme. AmSouth did not file a SAR on the accounts used by Nance and Hamric until nearly two years after the date that the suspicious activity should have been detected, and several months after AmSouth learned that law enforcement was investigating Hamric. By characterizing the suspicious activity as check fraud and understating the amount involved, the SAR failed to fully and accurately describe the criminal activities of Hamric. AmSouth's Legal Department, including its then-General Counsel, had reviewed the Hamric SAR after it was filed and found it sufficient.

While the Hamric activity was the predominant basis for the AmSouth prosecution, prosecutors pointed to several other instances where AmSouth should have filed SARs, but failed to do so. The failure to file SARs was indicative of serious deficiencies in AmSouth's AML program. In October 2004, AmSouth entered into a DPA and agreed to forfeit $40 million. The Information that was filed, charging one count of failing to file SARs, was dismissed in October 2005 pursuant to the DPA *v. AmSouth Bancorporation and AmSouth Bank*, No. 3:04-cr-167LSu (S.D. Miss. Oct. 12, 2004).

VI. Riggs Bank

Riggs Bank (Riggs) was convicted, pursuant to a guilty plea, of criminal violations of the BSA and ordered to pay a $16 million criminal fine, in addition to the $25 million civil penalty that had been previously imposed by FinCEN and the banking regulators. Riggs came to the attention of prosecutors in 2003 as a result of an investigation conducted by the Senate Permanent Subcommittee on Investigations into international political corruption and money laundering. The prosecutors found that Riggs failed to engage in even the most cursory due diligence review of accounts held by two particular customers—accounts known as "Politically Exposed Persons"—that Riggs knew posed a high risk of money laundering. Riggs allowed the accounts to be used to transfer large sums of money in a highly suspicious manner and failed to report such transactions to the proper authorities, as required by law. Moreover, the bank was aware of numerous obviously suspicious transactions—and in some cases executives at the bank even affirmatively assisted in conducting those transactions—yet failed to report them.

Riggs' failures involved, for the most part, banking relationships with Augusto Pinochet, the

former Chilean dictator, and the ruling family of Equatorial Guinea.

A. Pinochet accounts

Augusto Pinochet was the de facto leader or president of Chile from 1973 to 1990, the Commander-in-Chief of its armed forces, and sitting senator from 1990 to 1998. His rule was marked by allegations of significant human rights abuses and political corruption. In 1998, a Spanish magistrate issued an arrest warrant for Pinochet for crimes of genocide, terrorism, and torture, and issued a restraining order against all his assets. In November 1998, newspapers reported that U.S. authorities were discussing whether to seek the extradition of Pinochet in connection with the murder of two of his political opponents, by the Chilean secret police, in Washington, D.C. On January 29, 2001, Pinochet was placed under house arrest in Chile. By May of 2001, Pinochet's assets, held in various offshore accounts and investment vehicles, were being seized or frozen.

From 1985 to 2002, Pinochet and his wife, Lucia Hiriart Rodriguez, maintained multiple bank accounts, investments, and certificates of deposit at Riggs (collectively, the "Pinochet Accounts"). The Pinochet Accounts were located at Riggs in the United States and Riggs Bank Europe, Ltd., London, United Kingdom. Additionally, in 1996 and 1998, Riggs assisted Pinochet in the establishment of two offshore shell corporations in the Bahamas—Ashburton Company Ltd. and Althorp Investment Co., Ltd. Both were listed as nominal owners of bank accounts and certificates of deposit maintained by Pinochet.

During this time period, Pinochet deposited more than $10 million into his accounts at Riggs. Little due diligence was conducted on the source of Pinochet's wealth, and no attempt was made to reconcile his stated wealth with the subsequent deposits. Riggs employees and officers avoided using Pinochet's last name, even in routine internal communications, referring to him as "our prominent client in Chile," "the Washington client," or other aliases, including his wife's maiden name or his maternal family name.

Over the course of the history of the Pinochet Accounts, a number of suspect transactions were conducted by, or directed by, Pinochet. Riggs employees structured financial transactions in order to avoid the scrutiny of law enforcement and others who would seek to discover Pinochet's wealth. These transactions were highly unusual, suspicious, and appeared to be structured in a way to prevent their discovery by the OCC, law enforcement authorities, or others who may have been attempting to attach Pinochet's assets. Riggs Bank failed to conduct sufficient due diligence as to the source of the funds and failed to report any transactions that it knew, or had reason to know, were suspicious.

B. Equatorial Guinea

Equatorial Guinea (EG) is a country on the west coast of Africa that is approximately the size of Maryland. In 1995, billions of dollars of oil reserves were discovered within EG territorial waters, resulting in a significant influx of capital. Its President, Teodoro Obiang Nguema, came to power in 1979 in a military coup. His reelections in February 1996 and December 2002 were largely viewed by the United States government and international observers as tainted by fraud and intimidation. Public corruption had long been considered a significant problem in his government.

From 1996 to 2004, Riggs maintained numerous accounts for EG. Over the course of this period, Riggs opened over sixty-two accounts and certificates of deposit for the EG Government, numerous senior government officials, and their family members. Riggs opened multiple personal accounts for the President and his relatives and assisted in establishing offshore shell corporations for the President and his sons (known collectively as the EG Accounts). By 2003, the accounts had become Riggs's largest single relationship, with balances and outstanding loans that totaled nearly $700 million.

In September 1999, Riggs assisted the EG President in the establishment of Otong S.A., an offshore shell corporation, incorporated in the Bahamas. The Bahamas was a bank secrecy jurisdiction at the time of incorporation and held a money market account for the corporation. Over the course of the history of the EG Accounts, the following transactions took place through an account in the name of Otong S.A (the Otong Account).

- April 20, 2000: $1 million deposit of U.S. currency.
- March 8, 2001: $1.5 million deposit of U.S. currency.

- April 20, 2001: $1 million deposit of U.S. currency.
- September 5, 2001: $2 million deposit of U.S. currency.

Riggs failed to determine the background and possible purpose of these highly suspicious transactions. The bank also failed to file a SAR until after the OCC and Congressional investigators brought the transactions to the bank's attention. These transactions were suspicious because of the cash nature of the deposits, the lack of understanding as to the source or destination of the money, and the transactions were not the sort in which the particular customer would normally be expected to engage.

From April 2000 to April 2002, Riggs filed false CTRs on cash deposits that totaled $11.5 million made into one of the EG Accounts. These CTRs listed the Otong Account as an exporter of timber, rather than an offshore corporation controlled by the EG President. Certain Riggs employees knew this representation to be inaccurate.

In January 2005, Riggs pleaded guilty to failing to file an SAR in violation of 31 U.S.C. § 5318 and agreed to a fine of $16 million. Riggs was purchased by PNC Bank in May 2005, ending more than 160 years of Riggs' history in the District of Columbia. *United States v. Riggs Bank, NA,* No. Cr-05-35 (RMU) (D.D.C. Jan. 27, 2005).

VII. Bank of New York

In November 2005, the Bank of New York (BNY) entered into a nonprosecution agreement with the United States to resolve two separate investigations that were conducted in the Eastern and Southern Districts of New York. BNY admitted its criminal conduct and agreed to forfeit $26 million to the United States and pay $12 million in restitution to its victims. The bank also agreed to make sweeping internal reforms to ensure compliance with its antifraud and money laundering obligations, and be monitored by an independent examiner. BNY will not be prosecuted for the unlawful practices of its officers and employees for the following reasons.

- BNY's acceptance of responsibility.
- Its cooperation in the investigations.
- Its willingness to make restitution and take significant remedial action.

The bank must fully comply with the terms of its cooperation agreement with the government for a period of three years.

A. The Southern District of New York investigation

The investigation uncovered a scheme involving the unlicensed transmission of billions of dollars, originating in Russia, through BNY accounts in the United States, to third-party transferees. The investigation focused on misconduct related to the 1996 opening of accounts at a retail branch of BNY in the names of Benex International Co., Inc. (Benex) and BECS International LLC (BECS). These accounts were opened by Peter Berlin, a Russian émigré, with the assistance of his wife, Lucy Edwards, also a Russian émigré, who was a BNY vice president. During the next three and one-half years, approximately $7 billion flowed through the Benex and BECS accounts to third-party transferees around the world.

The Benex and BECS accounts were part of an underground money transfer business that was operated by a bank located in Moscow and a company located in Queens, New York. From an office in Queens, company employees executed hundreds of wire transfers each day from the Benex and BECS accounts, using electronic banking software provided by BNY. The instructions were provided by the Moscow bank.

Despite the obvious money laundering risks associated with such an operation, BNY failed to conduct adequate due diligence or make "KYC" inquiries with regard to Berlin or the Benex and BECS accounts. Some executives in the Retail Banking Division believed, incorrectly, that Berlin was in the import/export business, but no employee ever sought to verify that belief. Other executives in the Cash Management Division correctly understood that Benex and BECS essentially acted as payment brokers or money transmitters, whose businesses consisted solely of transferring funds on behalf of other parties. Those executives, however, did not make any inquiry as to whether Benex and BECS were properly licensed as money transmitters.

BNY also failed to adequately monitor the activity in the Benex and BECS accounts, which were the highest fee-producing accounts in the One Wall Street Branch. On the two occasions that Cash Management Division employees sought to conduct a money laundering review of

Benex and BECS accounts, they were advised by the Funds Transfer Division that BNY did not have an automated system for reviewing account activity. The manager further advised that it would be impractical to conduct a manual review of the accounts, given the tremendous volume of activity. A number of highly suspicious circumstances that should have raised flags about money laundering went undetected because of the failure to monitor the activity in these accounts.

In February 2000, Berlin and Edwards pled guilty to, among other crimes, conspiring to conduct unauthorized and unregulated banking activities, operate an illegal money transmitting business, and launder money to promote wire fraud. Berlin and Edwards acknowledged that the illegal banking network of which the Benex and BECS accounts were a part, was designed, in part, to allow Russian individuals and businesses to wire transfer funds in and out of Russia in violation of Russian currency controls, and thereby to defraud the Russian government of customs duties and tax revenues. *United States v. Peter Berlin and Lucy Edwards*, No. S1 99 Cr. 914 (SWK) (S.D.N.Y. Feb. 16, 2000).

B. The Eastern District of New York investigation

This investigation uncovered a scheme involving the submission of fraudulent loan applications, by a commercial customer, that were supported by sham escrow agreements executed by a corrupt BNY branch manager. This scheme resulted in millions of dollars in losses to victim banks throughout the United States. To date, at least nine individuals, including a former BNY vice president and a former BNY branch manager, have been convicted. The investigation disclosed that, from approximately 1991 to 2002, BNY branch managers and employees working at a retail branch in Island Park, New York, executed unauthorized and materially false and misleading escrow agreements for a BNY commercial customer, RW Professional Leasing Services Corp. (PLS). PLS was engaged in the business of arranging financing for medical providers, ostensibly for the leasing of medical equipment. Although the escrow agreements obligated BNY to act as an escrow agent for other banks that were financing the medical equipment leases, the bank deliberately failed to establish any escrow accounts or perform any terms of the escrow agreements. The financing banks relied on the escrow agreements in approving loan requests totaling tens of millions of dollars.

The scheme proceeded undetected for more than a decade and continued during the period that BNY was bound by the enhanced due diligence and reporting requirements of an agreement with federal and state banking regulators signed in February 2000. In early 2002, BNY executives learned of the illegal conduct at the Island Park branch. BNY's general counsel and managing counsel continued to ignore the bank's reporting obligations under the BSA and intentionally failed to take steps to file a SAR and notify law enforcement authorities in a timely manner.

In admitting responsibility, BNY acknowledged the following, among other things.

- It failed to have an effective AML program.
- It intentionally failed to take steps to report known evidence of suspected criminal conduct by a bank customer and BNY employees, as required under the mandatory reporting obligations of the BSA, even after that evidence came to the attention of senior BNY executives.
- The bank's general counsel, managing counsel, and other senior executives, repeatedly ignored the bank's legal obligations to file the required SARs.
- It filed SARs only after the principals of a BNY customer were arrested months later by federal authorities.

The SAR that was ultimately filed was both inaccurate and incomplete. It failed to make any reference to the misconduct of BNY personnel relating to the escrow agreements, or how the escrow agreements were used to defraud other banks. During this period, BNY was already under compulsion to correct problems in its AML program as a result of the Southern District of New York investigation, pursuant to an agreement between BNY, the Federal Reserve Bank of New York, and the New York State Banking Department. The agreement placed the bank under heightened regulatory scrutiny and required enhanced due diligence and suspicious activity reporting procedures by the bank. BNY's failures allowed the fraudulent activities to continue, resulting in at least $18 million in losses to victims.

VIII. BankAtlantic

In April 2006, Florida-based BankAtlantic entered into a DPA with the government and agreed to forfeit $10 million to resolve charges of failing to maintain an AML program. Concurrently, the Office of Thrift Supervision (OTS) and FinCEN each assessed a $10 million civil penalty against BankAtlantic for violations of the BSA, which was deemed satisfied by the payment of the $10 million forfeiture.

The charge filed against BankAtlantic arose out of transactions conducted by and through BankAtlantic between July 1997 and April 2004. During this time, more than $50 million in suspicious transactions were conducted through certain accounts, including transactions involving more than $10 million of identified drug proceeds. BankAtlantic failed to detect, identify, and report the suspicious transactions, as required by the BSA.

An undercover operation by the Drug Enforcement Administration into the laundering of drug proceeds found that $7 million of suspected drug money was being wire transferred to accounts at BankAtlantic. Further investigation led to the discovery of other accounts that were suspected of being used to launder drug money. These were accounts that either had received suspected drug proceeds or were related to those accounts or other accounts managed by the suspect who was the account manager.

These targeted accounts included the following characteristics which should have raised red flags at BankAtlantic.

- Accounts controlled by nonresident aliens, but held in the name of offshore shell corporations, particularly "bearer share" corporations, which are easily incorporated in such jurisdictions as the British Virgin Islands.
- Accounts controlled by domestic businesses that sell or export goods to South American customers, but generally receive payment from United States sources.
- Foreign MSBs that were determined to be unlicensed.
- Individual accounts held by nonresident aliens and U.S. residents being used to transmit funds for unrelated persons. These accounts are easily identified by numerous unrelated sources of incoming and outgoing transfers by check and wire.
- Licensed foreign MSBs that are operating by and through offshore shell corporations.

The targeted accounts were characterized by two types of activity that should have been readily identified as suspicious and reported by BankAtlantic.

- Most of the accounts showed a high volume of incoming and outgoing wire transfers from various domestic and international accounts held in the names of *unrelated* individuals and corporations.
- The accounts showed a high volume of check structuring activity.

Although the account manager personally handled most of the suspicious transactions, including the receipt of hundreds of pouch deposits containing sequential and structured checks, the account manager failed to take any action to report the suspicious activity, as required by the BSA.

The account manager not only failed to report the suspicious activity in the targeted accounts, but also concealed facts from bank management. The bank failed to maintain the required and necessary procedures and systems to *independently* identify and report suspicious activity. Serious and systemic AML and BSA compliance failures continued uncorrected at BankAtlantic for several years, some of which had previously come to the attention of law enforcement. Consequently, BankAtlantic admitted that it did not identify and report the suspicious activity occurring in these accounts, as required by the BSA. *United States v. BankAtlantic*, NO. 06-60126-CR-COHN (S.D. Fla. Apr. 26, 2006).

IX. American Express Bank International

In August 2007, American Express Bank International (AEBI), an Edge Act corporation headquartered in Miami, Florida, entered into a DPA with the Department and agreed to forfeit $55 million to resolve charges of failing to maintain an effective AML program. FinCEN assessed a $25 million civil money penalty and the Federal Reserve assessed a $2 million penalty (but the Federal Reserve penalty and $15 million

of the FinCEN penalty were deemed satisfied by the Department forfeiture).

The charge filed against AEBI arose from the same DEA investigation that resulted in the DPA against BankAtlantic. During this investigation, which took place between December 1999 and April 2004, investigators identified specific accounts (targeted accounts) at AEBI that they believed were used to launder more than $55 million of drug proceeds through the BMPE, a trade-based money laundering system through which South American money brokers facilitate a nonregulated currency exchange of United States dollars for local South American currency. The investigation disclosed that AEBI knowingly allowed South American customers to use accounts at the bank to process parallel currency exchange market transactions, many of which turned out to be BMPE transactions. These accounts were characterized by many suspicious incoming funds (typically wire transfers) from persons and entities completely unrelated to the account holder. In many cases, the financial transactions were inconsistent with the nature of the account holder's business, as understood by bank personnel. A large amount of funds was deposited into the accounts under circumstances suggesting that they were drug proceeds. In addition, hundreds of thousands of dollars of drug proceeds were transferred to these accounts directly from law enforcement agents, who in an undercover capacity, were "working for" Colombian money brokers and drug traffickers.

AEBI's particular risk to money laundering through parallel currency exchange transactions and the BMPE was heightened (1) because many of its clients were high net-worth residents in high risk countries in Latin America, such as Colombia, who often derived their wealth from commercial activities; (2) due to its character as an Edge Act bank engaged in providing private banking services to nonresident aliens; and (3) as a private bank. As early as November 1999, private banking was identified as a high-risk area in the fight against money laundering.

AEBI's compliance personnel were well aware of the prevalent use of the BMPE by Colombian businessmen and the nature of transactions which may be associated with the BMPE. Bank personnel demonstrated sophisticated knowledge and understanding of parallel currency exchange markets, in particular the BMPE. High-level bank officers were aware that South American parallel currency exchange markets had evolved into a system used to launder illicit proceeds and to bypass the government as the primary source of dollars to launder. Relationship Managers (RM) knew that it was common knowledge in South America, particularly Colombia, that the parallel exchange markets were funded, at least in part, with drug money and that there were two main reasons to use the parallel markets: 1) tax avoidance; and 2) a better exchange rate. At the same time, these AEBI RM's and supervisors considered the parallel exchange market a "fact of life" in South America—not something to be prevented or reported—but something that any financial institution providing banking services to wealthy South Americans would have to accommodate in the ordinary course of business.

The investigation of AEBI's compliance program determined that the primary cause of AEBI's failure to identify, prevent, and report this activity was that AEBI's AML program contained serious and systemic deficiencies in critical areas, as outlined below, which were uncovered during the investigation.

- AEBI failed to exercise sufficient control over accounts held in the names of offshore bearer share corporations, and until 2004 had no policy or procedure requiring beneficial owners of such accounts to certify in writing their continued ownership of the bearer shares.
- AEBI failed to conduct a risk assessment of its operations until 2002, and consequently was unable to, and did not, identify and monitor its highest-risk banking products and transactions.
- AEBI failed to develop and maintain an account monitoring program that was adequately designed to identify, detect, report, and prevent suspicious activities.
- AEBI failed to monitor adequately the source of funds sent to customer accounts to identify suspicious activities.
- AEBI failed to independently verify information on clients provided by private bank RMs.
- AEBI failed to provide compliance personnel with authority to identify and prevent suspicious and high-risk banking activities.

- AEBI failed to maintain an audit program reasonably designed to ensure the bank's compliance with BSA/AML laws and regulations.

A. Know your customer deficiencies

Almost all of the targeted accounts of AEBI shared the characteristic of being held in the names of "bearer share corporations" incorporated in offshore jurisdictions, such as the British Virgin Islands (BVI). Bearer share corporations are owned by the person or entity holding, or "bearing," the unregistered corporate common stock. There are no formal procedures for transferring ownership of a bearer share corporation's stock certificates, and linking any person to such a corporation is difficult. Accordingly, professional money launderers and other criminals frequently use such corporations to open offshore and domestic bank accounts to deposit illicit money. Bearer share structures make it extremely difficult for banks (and law enforcement) to determine the actual owners of accounts and to satisfy the KYC requirements.

One example among the targeted accounts at AEBI was an account controlled by a Colombian national, but held in the name of an offshore (BVI) bearer share corporation. This corporation was controlled by three other bearer share corporations, which had given the Colombian national a power of attorney, authorizing him to control the financial affairs and bank accounts of the original bearer share corporation. This individual processed millions of dollars in BMPE transactions through AEBI accounts.

In addition to the targeted accounts, the bank had numerous other accounts held in the names of offshore shell corporations, many controlled through bearer shares. Many of these accounts were beneficially owned and controlled by supposedly legitimate corporations in South America. There are few, if any, legitimate reasons why an established business concern would need or want to conduct financial transactions through secret accounts held in the names of offshore shell corporations. Yet, law enforcement has found that the presence of such accounts is endemic to international private banking in the United States, including AEBI.

B. AML risk assessment

AEBI was considered to be operating under a high risk of money laundering because of its location in south Florida, a designated High Intensity Drug Trafficking Area. Its provision of private banking services to high net-worth individuals living in Central and South America, a region known as a source for illegal narcotics, also put it at risk of money laundering. Yet no bank of substantial size can possibly monitor every single transaction and every single account. Thus, most banks conduct a formal and detailed risk assessment of each of its products, transactions, services, geographic locations, etc., and then tailor their limited AML and BSA resources to specifically monitor and control those areas identified as the highest risk. Prior to May 2002, AEBI did not conduct a risk assessment of its operations and products, and consequently failed to identify high-risk areas for enhanced monitoring.

C. Activity monitoring

The investigation also disclosed weaknesses in AEBI's account monitoring practices. AEBI relied upon a proprietary software system to monitor accounts for suspicious activity. This system, however, was only capable of identifying accounts that had breached preset parameters for external debits and total holdings, not for identifying suspicious activity patterns. The bank's written KYC policies and procedures set out a clear expectation that bank employees assess their client's transactions and ensure that those transactions remain consistent with the client's usual business and activities and make economic sense, based on their knowledge of the client's source of wealth and use of funds. To that end, AEBI RM's were tasked with conducting a monthly review of the activity occurring in all transaction accounts under their management, using *Activity Analysis Reports* and *Activity Detail Reports* distributed by Compliance, with the goal of identifying any activity which appeared to be out of pattern for the client or which required additional investigation. Law enforcement, however, identified a number of examples of red flag activity or suspicious activity that was unmonitored and unquestioned by AEBI, particularly with respect to the questionable source of funds from South American parallel currency exchange market activity. The primary cause of this failure is that AEBI's account monitoring system and the detail reports provided to the RM did not identify the country of origin or the source of incoming funds. This failure contributed significantly to the RM's failure to identify the massive amounts of parallel market transactions occurring in AEBI accounts.

Even in situations where accounts breached parameters and were flagged for review by the RM, the bank failed to effectively investigate the account activity. In general, the RM's were not given reports with sufficient transaction information to allow them to effectively review the activity in the account. On a number of occasions, instead of conducting further investigation, RM's simply informed Compliance that the activity in the account was consistent with the RM's knowledge of the client's business. No real review was conducted by the RM, and worse, Compliance did not independently look at the account activity to corroborate what the RM was reporting. Numerous similar examples were found at AEBI where RM's simply "explained away" parameter breaches, frequently requesting that Compliance increase the parameters on the accounts (apparently to avoid having to keep addressing the compliance issue each month).

The "Rules Based," as opposed to a "Risk Based," approach of monitoring activity, coupled with reliance on the RM to provide the assessment of the quality of account flows, without independent review and corroboration, was ineffective and caused AEBI to fail to identify, report, and prevent suspicious activity. Given that the account monitoring at AEBI was not a risk-based program, it was even more critical for AEBI's compliance personnel to independently review the account activity. Yet, the limited "independent reviews" conducted by Compliance were confined to those accounts that had exceeded external debit parameters. To the extent no exceptions were noted, all activity was deemed to be appropriate.

D. Independent review process

The situation at AEBI was further exacerbated by deficiencies in AEBI's independent review process. As part of AEBI's policies and procedures for account activity monitoring, Compliance personnel were supposed to perform spot checks or independent reviews of accounts that breached parameters. AEBI's compliance personnel maintained a log of the accounts reviewed and the results. This log recorded the name of the responsible RM, the account name, the parameter breached (holdings, activity-external debits, or both), and the comments or explanations of the activity causing the breach. A review of this log showed significant deficiencies in AEBI's "independent review" process.

AEBI's local compliance officer was permitted to exempt accounts from activity monitoring based only on the judgment of the compliance officer. Of the total number of accounts reviewed, the compliance officer had exempted 35.6 percent from the review process, many of which were commercial accounts held in offshore corporate names. There were some instances of accounts that had consistently breached parameters for over 21 months and went without review by Compliance for that same time. Compliance frequently justified the exemption based on the fact that the account was commercial in nature.

E. Prior enforcement activity

The compliance shortcomings at AEBI were especially disturbing because AEBI had previously been involved in a significant money laundering case and, consequently, was operating under the background of a Department of Justice Settlement Agreement. The Agreement relating to the Bank's compliance with the BSA and anti-money laundering regulations and statutes was entered into on November 18, 1994. The settlement grew out of a related indictment and conviction, in June 1994, of two of AEBI's employees, as a result of a U.S. Customs Service investigation into cartel leader Juan Garcia Abrego. *See United States v. Giraldi*, 86 F.3d 1368 (5th Cir. 1996); *United States v. Castaneda-Cantu*, 20 F.3d 1325 (5th Cir. 1994). This Settlement Agreement also followed a Cease and Desist Order and Civil Penalty between AEBI and the Federal Reserve dated November 1, 1993. As part of the Settlement, the Department withdrew and dismissed a civil money laundering complaint it had filed against AEBI and did not file criminal charges against the bank. AEBI also agreed to the following.

- A substantial monetary penalty, comprised of the withdrawal of AEBI's claim to a $30 million client account that served as collateral for $19 million in AEBI loans.
- The forfeiture of $7 million.
- A $7 million penalty.
- The bank agreed to spend no less than $3 million on the development and implementation of policies, procedures, and training, in order to assure compliance with the government's BSA/AML regulations and statutes.

Since the recent violations were disclosed at AEBI, the bank has devoted considerable resources to correct the identified BSA and AML deficiencies. Employees who failed to take vigorous action to support compliance efforts have either left AEBI or left their positions. AEBI has also identified, reported, and ultimately closed accounts used to process suspicious transactions, including each of the Targeted Accounts. AEBI has fully cooperated with the investigation and acknowledged responsibility for its actions. Consequently, the decision was made to resolve this case with a Deferred Prosecution Agreement (DPA). On August 6, 2007, a one-count Information was filed charging AEBI with failing to establish an AML program in violation of 31 U.S.C. § 5318(h). If AEBI is in full compliance with all of its obligations after one year, the government will move to dismiss the Information with prejudice.

X. Prosecutorial considerations

A. The Department's role

Why should prosecutors and investigators pursue an investigation of a financial institution for compliance shortcomings? These investigations are generally very complex, time consuming, and resource intensive. Should not the enforcement of an institution's AML compliance responsibilities be left to the financial regulators? AFMLS prosecutors are frequently asked these questions by the financial community and, occasionally, by the federal bank regulators.

Money laundering enforcement, perhaps uniquely, relies on many different entities to contribute. Each entity—prosecutors, law enforcement agencies, federal banking regulators, state banking regulators, the Treasury Department's FinCEN, and the industry itself—brings to the table unique knowledge, skills, and authorities to try to close off the U.S. financial system from money launderers. The system works when all cooperate toward the common goal.

The Department has an important role to play. In every one of the cases cited above, money laundering activity—potentially prosecutable under 18 U.S.C.§ 1957—took place through these institutions. This activity is very serious—so serious that, if a bank is convicted of a violation of § 1957, its federal regulator is required to hold a hearing to determine whether the bank should lose its license. While each of the cases discussed was resolved by a guilty plea, Deferred Prosecution Agreement, or Non-prosecution Agreement involving BSA charges, pursuant to the *Principles of Federal Prosecution of Business Organizations* (referred to as the *McNulty Memorandum* issued in December 2006), *available at* http://www.usdoj.gov/usao/eousa/foia_reading_room/usam/title9/crm00162.htm, the fact that there were potential money laundering charges in these cases made these cases significant and worthy of criminal enforcement actions. Moreover, a bank's failure to understand the source of its client's money often makes it difficult to show the specified unlawful activity necessary for a money laundering charge, or that the bank knew that the money was from some felonious source. Nevertheless, Congress felt sufficiently strongly about the issue that it provided for significant criminal penalties for willful violations of the BSA, itself.

The seriousness of the offense is due to the fact that significant harm can result from a bank's failure to live up to its responsibilities. As shown in these cases, a single lax branch of a bank, or even a single employee, can be responsible for millions in criminal proceeds being laundered quickly, safely, and cheaply. Underscoring the bank's obligations in this area, under threat of criminal sanction, ensures that banks will take seriously the need to be vigilant. Moreover, the threat of criminal prosecutions assists the bank regulators in their job. In that way, BSA enforcement is similar to other areas of the law where regulators and criminal prosecutors work in parallel, such as securities enforcement, with great effectiveness. Bank regulators have a number of sanctions available to them, and generally tailor the remedy to the seriousness of the problem. Some institutions, however, fail to correct their conduct, notwithstanding repeated warnings and penalties from the regulators. The OCC cited AML deficiencies in Riggs Bank, in over twenty-six different reports, but were unable to change the bank's practices in significant ways. In those circumstances, the Department steps in, as the regulator of last resort, with criminal sanctions.

B. Proving knowledge

Obviously, millions of dollars of criminal proceeds move through financial institutions every day. A bank cannot be held responsible for every transaction. An institution is criminally liable for money laundering charges under § 1957

only if it *knowingly* engages in a monetary transaction involving more that $10,000 in criminally-derived property. Under the principles of corporate criminal liability, the knowledge element for a corporation can be established either by showing a specific individual at a high enough level within the bank knew of, and furthered, the money laundering, or by showing the corporation's collective knowledge.

The concept of collective knowledge permits the government to prove knowledge of a corporate entity by offering evidence of the aggregate knowledge of the corporation's employees. *Bank of New England,* 821 F.2d 844, 855 (1st Cir. 1987) ("[Y]ou have to look at the bank as an institution. As such, its knowledge is the sum of the knowledge of all... [its] employees. That is,... the totality of what all the employees know..."). In the context of large corporations, which typically have highly compartmentalized structures, use of the collective knowledge doctrine is "not only proper but necessary." *Id.* at 856.

A corporation may be held criminally liable for conduct even though no single agent intended to commit the offense, or even knew the operative facts that constituted the violation. The intent and knowledge of various agents may be collectively attributed to the corporation, thereby giving rise to corporate liability where no individual criminal liability would exist. The court, in *Bank of New England*, instructed the jury that it could find that the corporation had knowledge of its filing obligations if any one of its individual employees had the requisite knowledge, or it could be inferred from the collective knowledge of all of its employees.

The concept of willful blindness allows the government to satisfy the knowledge requirement of a federal criminal statute by demonstrating that a defendant willfully, consciously, and/or deliberately avoided knowledge of certain facts essential to proof of a criminal violation. The First Circuit has approved the concept of willful blindness against a corporate defendant in a BSA prosecution. In this context, the government may prove corporate *mens rea* by demonstrating organizational indifference to wrongdoing by corporate employees. "Flagrant organizational indifference," *id.* at 855, can satisfy the wilfulness requirements. The court, in *Bank of New England*, held that it was proper for the district court to instruct the jury that it could infer culpable knowledge if it found that the bank had consciously avoided learning about the currency transaction reporting requirements as a result of some "flagrant organizational indifference." *Id.*

The government may show "flagrant organizational indifference" to the requirements of the law by the following evidence.

- The bank's failure to adequately inform its employees of the legal duty to report.
- The bank's failure to implement an effective compliance program.
- The bank's failure to properly respond to information it received relating to the reporting requirements.
- The bank's own stated policies or its failure to implement those policies.
- The bank's response to various bits of information it received

If this information adds up to flagrant organizational indifference to the reporting requirements, it supports a finding of willfulness as well. *Id.*

C. Factors to consider in prosecutions

The Department does not target specific financial institutions for prosecution. In every one of the cases cited above, the bank's conduct aroused the attention of prosecutors and investigators who were investigating other criminal activity. Attention turned to the bank during the course of the investigation as a result of the bank's conduct within the scope of the criminal activity under investigation, or as a result of the bank's conduct during the course of the investigation. When initial scrutiny of the bank's conduct raised serious concerns about its activity and compliance shortcomings, the investigations proceeded into full criminal investigations.

Once a criminal investigation begins, several factors are considered in assessing whether an institution's violation of the BSA warrants criminal remedies. Each of these factors is reflected in the investigations described above, and there is every reason to believe that these are the factors that prosecutors will continue to look to in evaluating cases in the future.

- *The violation must be willful.* A criminal violation of the BSA must involve evidence (beyond a reasonable doubt) that a decision was "willful," that is, the bank understood its obligations under the BSA and, nevertheless,

deliberately decided to violate the law. This is the highest burden the law allows and, as prosecutors, we are mindful that the criminal law is not a law of negligence.

- *The decision whether to file a SAR is a judgment call.* Under the BSA, a financial institution is required to file a SAR where it "knows, suspects, or has reason to suspect one of the following."
    - That after an appropriate investigation, the financial institution determined that it is a transaction with no apparent business purpose, or is not the sort that the customer would be expected to engage in.
    - That it is derived from illegal funds or designed to hide the origin of the funds.

Since this is not a clearly objective standard, the government would need strong and compelling evidence that the transactions in question were suspicious, and that the institution, in fact, knew they were suspicious, in order to prove a criminal violation.

- *There must be evidence of a systemic failure.* The government will look closely at whether the financial institution has a healthy and effective AML program. If the bank has a program to find potentially suspicious activity, and after researching the transactions involved determines that no SAR need be filed, it would be extremely rare for the government to second-guess that decision, even if the decision was clearly wrong. However, where the bank fails to even know about the transaction as a result of a poor AML program, the government will be far less sympathetic. Most prosecutions of institutions for BSA violations have centered on this factor.

What does an effective compliance program look like? In the Department's view, the U.S. Sentencing Commission has put forth the best description of an effective compliance program in section 8B2.1 of the *United States Sentencing Guidelines*. Some of the operative factors include the involvement of high-level personnel in the operation of the program, appropriate incentives to employees to ensure effective compliance, as well as education and independent testing of the effectiveness of the program. The mere existence of a paper program is insufficient. Prosecutors will not hesitate to investigate whether a compliance program has any teeth.

- *The bank has a duty independent of its regulator.* While regulators periodically assess an institution's AML program, the BSA makes clear that the responsibility for determining whether the program is effective rests on the institution, not the regulator. Prosecutors will consider whether an institution received favorable reports from its regulator, but will also look behind those reports to determine whether such clean bills of health were reasonable. In a number of instances, prosecutors have found no justification for a regulator's conclusion of a satisfactory AML program and, as such, have given it little weight.

As a result of this analysis, financial institutions that take their obligations seriously, and that fund and maintain a real AML program, are well positioned to avoid criminal scrutiny for a BSA violation. Institutions that do not take their obligations seriously may face a criminal enforcement action if their conduct should come within the scope of a criminal investigation.

XI. Conclusion

Banks are the principal gateway into the U.S. financial system and have been given major responsibilities for safeguarding that gateway and trying to detect and prevent criminal proceeds, or terrorism funds, from entering the financial system. These responsibilities are imposed by law, and there must be sanctions for failing to fulfill these responsibilities. Whenever it is determined that a significant amount of criminal proceeds are flowing into or through a financial system, it should be examined to determine if it has effective AML policies and practices, or whether the institution is shirking its duties. If it is the latter, then the seriousness of the violations should be considered to determine whether a civil or criminal enforcement action is warranted.

Pursuant to § 9-105.300 of the *United States Attorneys' Manual,* in any criminal case under 18 U.S.C. §§ 1956 or 1957 or 31 U.S.C.§ 5322, in which a financial institution, as defined in 18 U.S.C. § 20 and 31 C.F.R. § 103.11, would be named as a defendant, or in which a financial institution would be named as an unindicted coconspirator or allowed to enter into a Deferred Prosecution Agreement, Criminal Division approval through AFMLS is required before any indictment, complaint, information, or Deferred Prosecution Agreement is filed. The attorneys in

AFMLS should be consulted when such investigations are initiated. They can be reached at 202-514-1263.❖

ABOUT THE AUTHORS

❑**Lester M. Joseph** is the Principal Deputy Chief in the Asset Forfeiture and Money Laundering Section (AFMLS). He has been a Deputy Chief since the Money Laundering Section was created in 1991. He became Principal Deputy Chief in January 2002. Mr. Joseph joined the Department in 1984 as a Trial Attorney in the Organized Crime and Racketeering Section. From 1981 to 1984, he was an Assistant State's Attorney in Cook County (Chicago), Illinois.

❑**John Roth** is the Chief of the Fraud and Public Corruption Section for the U.S. Attorney's Office in the District of Columbia. He is the former Chief of the Asset Forfeiture and Money Laundering Section, as well as the Narcotic and Dangerous Drug Section of the Department's Criminal Division. Mr. Roth joined the Department in 1987 as an Assistant U.S. Attorney in the Eastern District of Michigan. He then served in the Southern District of Florida, as Chief of the Narcotics Section. He is currently detailed to the Criminal Division as an acting Deputy Assistant Attorney General, responsible for narcotics and money laundering enforcement.✠

NOTES

Request for Subscription Update

In an effort to provide the UNITED STATES ATTORNEYS' BULLETIN to all federal law enforcement personnel who wish to receive it, we are requesting that you e-mail Nancy Bowman (nancy.bowman@usdoj.gov) with the following information: Name, title, complete shipping address, telephone number, number of copies desired, and e-mail address. If there is more than one person in your office receiving the BULLETIN, we ask that you have one receiving contact and make distribution within your organization. If you do not have access to e-mail, please call 803-705-5659. Your cooperation is appreciated.