

## Banking on Compliance

By Leonard L. Gumpert

The operator of a Ponzi scheme typically needs at least one bank account. The operator uses that account to deposit duped investors' funds, to commingle them, to extract personal fees and operating expenses (including maintenance of the scheme's facade as a legitimate business) and to pay redemptions and fictitious profits to investors. When the scheme collapses, the operator is always insolvent and sometimes in jail.

Investor-victims who lost their money in a Ponzi scheme may ask whether they have claims against the former operator's bank depository. While investor-victims investigate their possible claims against the bank, the news of the scheme's collapse requires the bank to file within 30 days a suspicious activity report with the Treasury Department's Financial Crimes Enforcement Network. At the same time, the bank must evaluate how the Ponzi scheme operated from an account at the bank despite its Bank Secrecy Act and anti-money laundering compliance programs.

As a general rule, "under California law, a bank owes no duty to nondepositors to investigate or disclose suspicious activities on the part of an account holder." *Casey v. U.S. Bank National Association*, 127 Cal.App.4th 1138 (2005). As *Casey* discusses, however, a bank may be held liable for aiding and abetting its customer's intentional wrongdoing, if the bank actually knew about the wrongdoing and substantially assisted it. *Casey* involved claims by the bankruptcy trustee of a corporation against banks that provided services to officers and directors of the corporation. The trustee alleged that the banks aided and abetted the officers and directors in breaching their fiduciary duties to the corporation by siphoning, through nominee accounts at the banks, \$36 million of the \$47.6 million that the corporation had raised from investors. *Casey* applied a strict pleading standard, scrutinizing the sufficiency and specificity of the complaint's aiding and abetting allegations. The trustee's allegations that the banks knew of suspicious activities, even possible money laundering, did not adequately allege that the banks actually knew that the officers and directors wrongfully diverted the corporation's funds through the nominee accounts at the banks. *Casey* reasoned that its strict pleading standard reconciled two distinct legal principles, "one that strictly limits a bank's duties to nondepositors and another that

extends tort liability to anyone who knowingly aids and abets the tort of another." Because the trustee's allegations against the banks were conclusory, *Casey* ruled that the trial court correctly sustained the banks' demurrers, but reversed the judgment and remanded the case to give the trustee an opportunity to

**The bank must evaluate how the Ponzi scheme operated from an account at the bank despite its Bank Secrecy Act and anti-money laundering compliance programs.**

amend. Because the trustee had not alleged that the officers and directors of the corporation were its sole decision-makers, the otherwise obvious and dispositive defenses of unclean hands and in pari delicto did not apply.

*Casey* relied on *Neilson v. Union Bank of California N.A.*, 290 F.Supp.2d 1101 (C.D. Cal. 2003), in analyzing the aiding and abetting liability of banks. In the context of a motion to dismiss, *Neilson* ruled that banks could be liable to investor-victims of a Ponzi scheme on causes of action for aiding and abetting the Ponzi operator's fraud and breaches of fiduciary duty. *Neilson* and *Casey* differentiated between civil conspiracy and aiding and abetting, which requires neither a conspiracy nor an independent duty between the aider/abettor and the victim. The elements of aiding and abetting liability are the intentional tort of the primary tortfeasor, the aider and abettor's actual knowledge of the tort and the aider and abettor's deliberately providing substantial assistance or encouragement to the primary tortfeasor in committing the tort. See *In re First Alliance Mortgage Company*, 471 F.3d 977 (9th Cir. 2006); *Zonzales v. Lloyds TSB Bank PLC*, 532 F.Supp.2d 1200 (C.D. Cal. 2006).

Evaluating whether a bank knew of its customer's Ponzi scheme requires familiarity with the Bank Secrecy Act and its implementing

regulations, because they require a bank to have systems to identify and report suspected illegal transactions at the bank. In 1992, Congress amended the act by enacting the Annunzio-Wylie Anti-Money Laundering Act, which authorized the Treasury Department to require banks to report suspicious transactions. Thereafter, bank regulators, including the Financial Crimes Enforcement Network and the Office of the Comptroller of the Currency, issued regulations that require banks to prepare and file a suspicious activity report with regulators, generally within 30 days of detecting a suspicious transaction at the bank. See, e.g., 12 Code of Federal Regulations Section 21.11; 31 Code of Federal Regulations Section 103.18. In 2001, Congress further amended the Bank Secrecy Act by enacting the USA PATRIOT Act, which required banks to have anti-money laundering programs.

A bank's Bank Secrecy Act compliance program must, at a minimum, meet four requirements. First, it must provide for a system of internal controls to assure compliance, including compliance with the duty to report knowledge and suspicions of illegal transactions. Second, it must provide for independent testing for compliance to be conducted by bank personnel or by an outside party. Third, the program must designate an individual or individuals responsible for coordinating and monitoring day-to-day compliance. Lastly, the program must provide training for appropriate personnel. A bank's anti-money laundering program must meet similar requirements.

A suspicious activity that a bank must timely report includes, among other things, any transaction involving at least \$5,000 and that the bank "knows, suspects, or has reason to suspect" involves funds derived from illegal activities or is intended or conducted in order to hide or disguise funds or assets derived from illegal activities as part of a plan to violate or evade any federal law or regulation or to avoid any transaction reporting requirement under federal law or regulation. A Ponzi scheme by definition involves funds derived from illegal activities, including mail or wire fraud.

A bank that fails to comply with the Bank Secrecy Act and its regulations risks regulatory and criminal proceedings. For example, a total of \$50 million in fines and penalties were assessed against AmSouth Bank of Birmingham, Ala. and its corporate parent for violations, including failures to file suspicious activity reports relating to the operation of a Ponzi scheme from accounts at the bank. AmSouth's



Bank Secrecy Act-related programs are described in *Stone v. K.A. 2d 362 (Del. 2006)*.

Investor-victims are not to subpoena suspicious reports from the former operator's bank. The reports made confidential and protected by banking regulations that meant 31 U.S.C. Section 5420. The regulations create a privilege and evidentiary privilege courts have held cannot be waived. See *Union Bank of California v. Superior Court*, 130 Cal.App.4th 1138 (2005), quoting *Whitney Bank v. Karam*, 306 F.Supp.2d 1200 (S.D. Texas 2004).

Although a suspicious activity report is privileged, not all documents are shielded from discovery, including wire transfers, checks and deposits. Examples of the types of documents generated in the ordinary course of business that are subject to discovery by private litigants under the Code of Federal Regulations include a mechanism to request nonpublic information from the Office of the Comptroller of the Currency, including suspicious activity report nonpublic information.

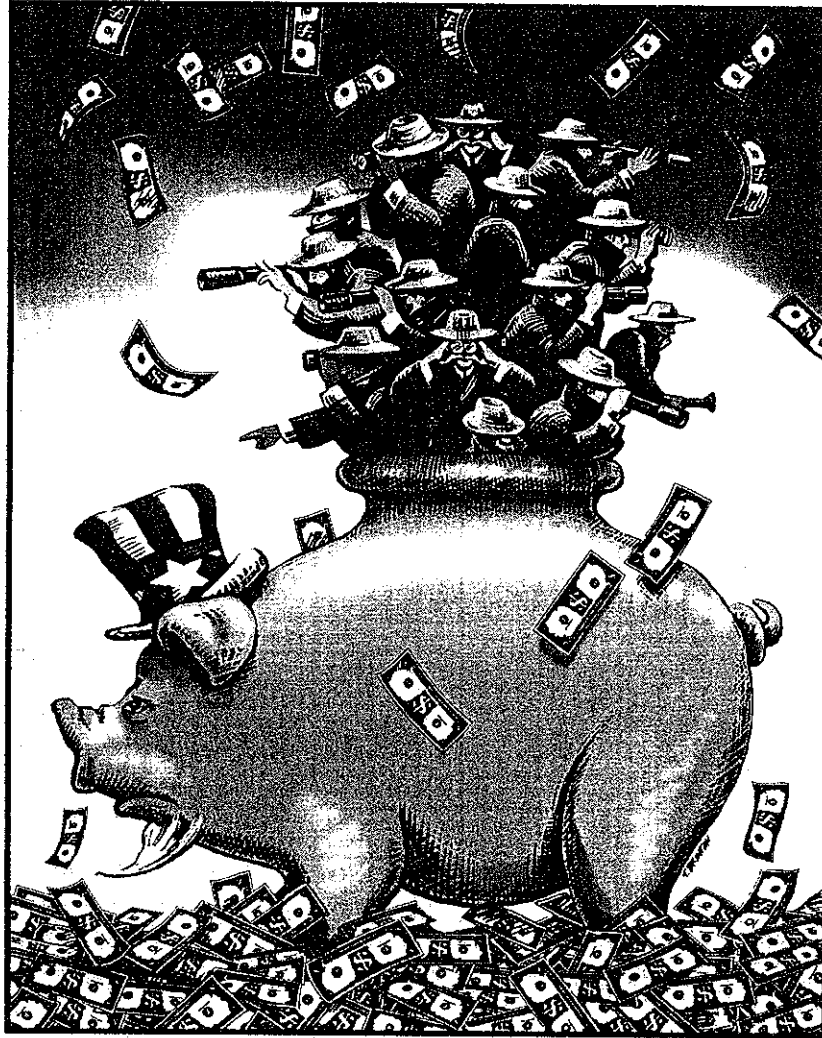
## Compliance

regulations, because they require a bank to have systems to identify and report suspected illegal transactions at the bank. In 1992, Congress amended the act by enacting the Annunzio-Wylie Anti-Money Laundering Act, which authorized the Treasury Department to require banks to report suspicious transactions. Thereafter, bank regulators, including the Financial Crimes Enforcement Network and the Office of the Comptroller of the Currency, issued regulations that require banks to prepare and file a suspicious activity report with regulators, generally within 30 days of detecting a suspicious transaction at the bank. See, e.g., 12 Code of Federal Regulations Section 21.11; 31 Code of Federal Regulations Section 103.18. In 2001, Congress further amended the Bank Secrecy Act by enacting the USA PATRIOT Act, which required banks to have anti-money laundering programs.

A bank's Bank Secrecy Act compliance program must, at a minimum, meet four requirements. First, it must provide for a system of internal controls to assure compliance, including compliance with the duty to report knowledge and suspicions of illegal transactions. Second, it must provide for independent testing for compliance to be conducted by bank personnel or by an outside party. Third, the program must designate an individual or individuals responsible for coordinating and monitoring day-to-day compliance. Lastly, the program must provide training for appropriate personnel. A bank's anti-money laundering program must meet similar requirements.

A suspicious activity that a bank must timely report includes, among other things, any transaction involving at least \$5,000 and that the bank "knows, suspects, or has reason to suspect" involves funds derived from illegal activities or is intended or conducted in order to hide or disguise funds or assets derived from illegal activities as part of a plan to violate or evade any federal law or regulation or to avoid any transaction reporting requirement under federal law or regulation. A Ponzi scheme by definition involves funds derived from illegal activities, including mail or wire fraud.

A bank that fails to comply with the Bank Secrecy Act and its regulations risks regulatory and criminal proceedings. For example, a total of \$50 million in fines and penalties were assessed against AmSouth Bank of Birmingham, Ala. and its corporate parent for violations, including failures to file suspicious activity reports relating to the operation of a Ponzi scheme from accounts at the bank. AmSouth's



Bank Secrecy Act-related problems are described in *Stone v. Ritter*, 911 A.2d 362 (Del. 2006).

Investor-victims are not entitled to subpoena suspicious activity reports from the former Ponzi operator's bank. The reports are made confidential and privileged by banking regulations that implement 31 U.S.C. Section 3518(g). The regulations create what has been called "an unqualified discovery and evidentiary privilege that courts have held cannot be waived." *Union Bank of California N.A. v. Superior Court*, 130 Cal.App.4th 378 (2005), quoting *Whitney National Bank v. Karam*, 306 F.Supp.2d 678 (S.D. Texas 2004).

Although a suspicious activity report is privileged, not all underlying documents are shielded. Transactional and account documents, including wire transfers, bank statements, checks and deposit slips, are examples of the types of documents generated in the ordinary course of business that are subject to civil discovery by private litigants. Further, the Code of Federal Regulations provides a mechanism for litigants to request nonpublic information from the Office of the Comptroller of the Currency, including suspicious activity reports and other nonpublic information concerning

banks under regulatory supervision. The Office of the Comptroller of the Currency's regulations include a Model Protective Order that the office requires in those circumstances where it chooses to release otherwise confidential information.

A bank's sloppy errors and suspicions that "something fishy was going on" do not, without more, make the bank an aider and abettor of its customer's intentional wrongdoing. A bank's mere non-compliance with the Bank Secrecy Act and its regulations does not mean that the bank knowingly and substantially assisted its customer's intentional wrongdoing as required for aiding and abetting liability. *Mazzaro de Abreu v. Bank of America Corporation*, 525 F.Supp.2d 381 (S.D.N.Y. 2007). Under *Casey*, "ordinary business transactions" performed by a bank can constitute aiding and abetting under California law, provided that the bank actually knew of the underlying intentional tort and substantially assisted it. In arriving at this conclusion, *Casey* acknowledged conflicting precedent outside California.

When a bank systematically violates its duties to file suspicious activity reports and to implement a compliance program, then the

bank should expect law enforcement and regulators to reveal the bank's misconduct in regulatory or criminal proceedings against the bank. While some regulatory violations are resolved confidentially, the Financial Crimes Enforcement Network Web site includes information about banks that were publicly sanctioned. When disclosures of a bank's systematic Bank Secrecy Act violations occur in a regulatory or criminal proceeding against the bank concerning its handling of a Ponzi operator's bank account, investor-victims may disbelieve the bank's denials of aiding and abetting the operator. For that reason, among others (including the civil and criminal penalties that can result to the bank from violating the Bank Secrecy Act), it is in the bank's interest to diligently comply with the act and to implement an adequate compliance program.

Leonard L. Gumport is a partner in Gumport Reitman. He has served as a bankruptcy trustee, SIPC trustee, bankruptcy examiner, provisional director and special counsel to public and private entities in internal investigations. The firm has represented trustees in Ponzi scheme-related cases, including some related to cases cited in this article.