

Ponzi Schemes and Bank Liability: The New “Red Flags,” the Risks and the Decision Whether To Terminate the Customer Relationship

GORDON A. GREENBERG AND HOYT Y. SZE

The authors explore what a bank should do when confronted with “red flags” indicating that a customer might be operating a Ponzi scheme.

Throughout this past year, Ponzi schemes have been a leading news topic. First, in December 2008, Bernard Madoff’s \$50 billion investment advisor Ponzi scheme was exposed when Madoff told a few employees about the details of his fraudulent scheme.¹ Then, in February 2009, the Securities & Exchange Commission (“SEC”) uncovered R. Allen Stanford’s alleged \$8 billion certificate of deposit Ponzi scheme.² Throughout 2009, many more revelations of “Ponzi schemes” permeated the news so much so that Charles Ponzi, the namesake of the scheme, would have presumably been startled at his infamy.³

A Ponzi scheme is defined as an operation that uses the principal received from new investors to make payments to initial investors, such payments being falsely characterized as returns or profits. In addition to the “rob-Peter-to-pay-Paul” aspect, some other usual hallmarks of a Ponzi scheme include advertising high returns, misappropriating of investor funds for personal uses or uses unrelated to stated purposes and commin-

Gordon A. Greenberg and Hoyt Y. Sze are partners in the Trial Department of McDermott Will & Emery, resident in the firm’s Los Angeles office. They can be reached at ggreenberg@mwe.com and hsze@mwe.com, respectively.

gling of investor funds with other monies. Although Ponzi schemes are not new, both Madoff's and Stanford's fraudulent practices continued for years without government intervention.

What is a bank to do when confronted with "red flags" indicating that a customer might be operating a Ponzi scheme? First, as explained below, the Bank Secrecy Act and related regulations may impose a duty on the bank to file a Suspicious Activity Report ("SAR") and to incorporate such "red flags" in its compliance program. Second, these "red flags" have become increasingly important as victim investors have filed lawsuits against the banks utilized by Ponzi scheme operators alleging that such banks have aided and abetted the underlying fraud.⁴ Even though some courts have ruled that a bank's knowledge of mere improprieties or atypical banking procedures or the bank's failure to act in the face of a single or isolated "red flags" might not lead to civil liability, other courts have permitted such cases to survive motions and go to trial despite the risk and expense to the banks. The intersection of a bank's obligations under the Bank Secrecy Act and its desire to avoid civil liability creates a minefield of risks that must be carefully maneuvered. Before describing that minefield, we begin by describing some of the "red flags" alleged by plaintiffs' counsel in recent lawsuits against banks for their role in purportedly aiding and abetting Ponzi schemes.

RED FLAGS

The Bank Secrecy Act/Anti-Money Laundering ("BSA/AML") Examination Manual issued by the Federal Financial Institutions Examination Council ("FFIEC") and revised in 2007 lists 8 pages of money laundering red flags.⁵ Some of the more familiar of the red flags listed in the Examination Manual include: customers who provide insufficient or suspicious information, customers who are reluctant to comply with reporting or record-keeping requirements, funds transfers to or from a financial secrecy haven, unusual transfers of funds between related entities, sudden inconsistencies in currency transaction patterns and shell company activities.

However, in recent civil litigation against banks for aiding and abetting Ponzi schemes and other fraud, plaintiffs' counsel have identified additional potential red flags for banks, including the following:

- Suspicious intracompany transfers and other banking activity by a company combined with establishment by a bank of a branch office in the company's offices where due to electronic connection between the bank and company's systems, bank representatives could monitor all banking activity of the company.⁶
- Criminal history of company's principals combined with company's lack of legitimate business activities, irregular documentation, bank employee visits to discuss company's business and majority of bank branch employees simultaneously working at the company.⁷
- Banking procedures that violated internal rules combined with personal or business ties between the bank and company such as overlapping boards of directors or bank employees who were relatives of the company's principal.⁸
- Discovery by a bank of prior criminal history of a company principal, litigation accusing the company of wrongdoing or regulatory enforcement activity concerning the company.⁹
- Continued provision of banking services by bank to company even after bank conducted diligence on company's operations and decided to liquidate bank's own position in company's investment funds.¹⁰
- Diversion of funds to accounts not listed in deposit instructions.¹¹
- Diversion of funds to personal commodities trading accounts.¹²
- Attendance by bank representatives at investor meetings where misrepresentations as to bank's role were made.¹³
- Institution of unusual systems by a bank necessary to ensure against repeated "bouncing" of checks by company.¹⁴

The identification by a bank of one or more of these red flags may require the bank to conduct necessary actions under the Bank Secrecy Act and/or to take measures to limit exposure to civil liability.

BANK SECRECY ACT

The Bank Secrecy Act may impose important obligations on a bank confronted by one of these red flags.

First, the Bank Secrecy Act requires banks to file a Suspicious Activity Report (“SAR”) with respect to any transaction involving at least \$5,000 which the bank suspects “involves funds derived from illegal activities” or “has no business or apparent lawful purpose.”¹⁵ It is important to note how broad this obligation extends. The Bank Secrecy Act may be aimed at detecting potential money laundering but the activity that might trigger a SAR is not limited to obvious criminal activity such as drug trafficking or terrorism. The potential civil and criminal penalties for a violation of the Bank Secrecy Act can be severe and can include removal from banking. For example, a willful violation of the Bank Secrecy Act is punishable by a criminal fine of up to \$250,000, or five years in prison, or both, as well as criminal monetary penalties of up to \$1 million or twice the value of the transaction.¹⁶ Some recent well-known examples of punishments for failure to file SARs include the January 2005 \$25 million civil fine against Riggs Bank, N.A. for its handling of funds of Chilean dictator Augusto Pinochet and the November 2004 \$50 million civil fine/forfeiture against AmSouth Bank for its services provided on behalf of customers who turned out to be operating a Ponzi scheme.¹⁷

Second, the Bank Secrecy Act requires a bank to adopt a written board approved program designed to assure and monitor compliance with the Act.¹⁸ Among other things, the compliance program must provide for a system of internal controls to ensure ongoing compliance.¹⁹ Pursuant to the BSA/AML Examination Manual, the FFIEC continuously assesses the ongoing effectiveness of the requisite system of internal controls.²⁰ Therefore, even though “red flags” might be unusual or not listed in the Examination Manual, a bank might be required to incorporate risky or recurring “red flags” into its compliance program.

Complicating the bank’s decision even further is the potential for civil lawsuits filed by victim investors after the bank acts or chooses not to act after discovery of one of these “red flags.”

AIDING AND ABETTING LIABILITY FOR BANKS

Increasingly, victim investors have filed class action lawsuits alleging that banks aided and abetted Ponzi scheme companies in perpetrating fraud. In both the Madoff and Stanford cases, for example, the victim investors have sued the banks which provided services for Madoff and Stanford's businesses.²¹ In most states, to prove aiding and abetting fraud, a plaintiff must show three elements: the existence of a fraud, the defendant's actual knowledge of the fraud and that the defendant provided substantial assistance to advance the fraud's commission.²² Recent developments in the caselaw on these elements provide a bank with helpful defenses to the last two elements of aiding and abetting; namely, knowledge and substantial assistance. However, these defenses are imperfect and fact-dependent. A bank in this situation should be loathe to take no action after learning of one of these "red flags" in the hopes that a "no knowledge" or "no substantial assistance" defense will ultimately prevail, particularly in light of the Bank Secrecy Act obligations described above.

Each of these defenses described above may not adequately protect a bank that takes no action in light of one of these red flags.

No Knowledge Defense

Courts have ruled that to adequately allege aiding and abetting liability, a plaintiff must allege actual knowledge of the underlying fraud. Actual knowledge of mere improprieties or atypical banking procedures is not sufficient to plead aiding and abetting fraud.

The clearest example of this is *Casey v. U.S. Bank National Association*, a California state court decision, which involved a bankruptcy trustee's claim that several banks aided and abetted the fiduciaries of a debtor corporation in looting assets from the debtor corporation.²³ The trustee alleged that the banks permitted the fiduciaries to open accounts for entities the bank knew to be illegitimate, the banks knew that the fiduciaries were using forged checks and checks whose limits were exceeded to withdraw funds from the accounts, and the fiduciaries carried "large, unreported amounts of cash" out of the bank in unmarked duffel bags."²⁴ Even though these alleged facts showed that the bank knew "something

fishy was going on,” they did not adequately allege the bank’s knowledge of the fiduciaries’ misappropriation of the debtor corporation’s funds.²⁵ Similarly, several courts have held that even if a bank is on notice as to atypical banking procedures, this is not sufficient to allege knowledge.²⁶

Confronted by one of the “red flags” described above, a bank should not overly rely on a “no knowledge” defense on the grounds that it only knew of improprieties or atypical banking procedures rather than outright fraud. As to improprieties, the bright-line rule in *Casey* is not always followed in practice even in California. Although not directly contradicting *Casey*, California courts in published and unpublished decisions have determined that plaintiffs adequately pled actual knowledge by alleging knowledge of mere improprieties.²⁷ Moreover, due to the broad scope of the Bank Secrecy Act, a bank may have to file a SAR even with respect to “red flags” that appear to be mere improprieties. (It should be noted that, although the facts underlying the SAR are not confidential, the filing of a SAR itself is confidential under the Bank Secrecy Act and thus cannot be subpoenaed by plaintiffs to establish knowledge).²⁸

As to atypical banking procedures, this defense is also not consistently applied by the courts. For example, a federal court in California found that an allegation that a bank “utilized atypical banking procedures” was sufficient to allege actual knowledge.²⁹ Similarly, in a recent case in Cleveland, a federal court permitted a plaintiff’s case against a bank for aiding and abetting a Ponzi scheme to go to trial when the plaintiff only alleged that the bank took actions that violated its own internal procedures combined with a bank employee being the daughter of the Ponzi scheme operator.³⁰ Although the jury in Cleveland ultimately found in favor of the bank, the bank was forced to undergo the risk and expense of trial.

Thus, a bank confronted with “red flags” indicating a Ponzi scheme should take little solace in a “no knowledge” defense based on the theory that it only knew of improprieties or atypical banking procedures, rather than actual fraud.

Failure to Act Defense

Courts have also increasingly ruled in this context that, absent a fiduciary duty, a bank’s mere failure to act ordinarily does not satisfy the “sub-

stantial assistance” element of aiding and abetting liability.³¹ This defense is based on the fact that, ordinarily, a “bank owes no duty to nondepositors to investigate or disclose suspicious activities on the part of an account holder.”³² However, a bank’s decision to take no action with respect to a “red flag” is not automatically protected from liability due to this “failure to act” defense. First, as described above, a bank’s failure to file a SAR after learning of such a “red flag” might be a violation of the Bank Secrecy Act which could involve dire consequences. (Frequently, plaintiffs’ attorneys have referred to the Bank Secrecy Act and its anti-money-laundering provisions as standards of care, departures from which are alleged to be acts of aiding and abetting).³³ Second, in California at least, as long as the bank has actual knowledge of the underlying fraud, the bank’s provision of even ordinary banking services can constitute substantial assistance.³⁴ Thus, in California, the “failure to act” defense might not protect a bank from civil liability if it continues to provide ordinary banking services to a customer that it knows might be operating a Ponzi scheme. Third, with respect to fiduciary accounts like attorney trust accounts, courts have declined to apply this “failure to act” defense, reasoning that once the defendant bank learned of misappropriation of trust funds, it was obligated to act.³⁵ Thus, the failure to act defense does not even apply to bank’s administration of certain fiduciary accounts.

In sum, despite these recent helpful developments in the caselaw, a bank should not decide to act or not act once it learns of one of these “red flags” in the hopes that relying on one of the imperfect defenses described above can ensure against risk of civil liability.

TERMINATING THE CUSTOMER RELATIONSHIP

The logical next question with respect to one of these “red flags” is whether to terminate the customer as a client of the bank. Unfortunately, neither the Bank Secrecy Act nor its related regulations provides any guidance as to this decision. While the Bank Secrecy Act provides a safe harbor, that safe harbor arguably only protects against liability for the filing of the SAR rather than any actions taken by the bank after the filing.³⁶

Likewise, the decision whether to terminate the customer relationship

involves both civil and criminal liability risk. On the one hand, termination of the client relationship could subject the bank to a civil lawsuit by the customer.³⁷ On the other hand, in recent litigation, plaintiffs' lawyers have repeatedly alleged that a bank's failure to terminate a customer relationship (especially when others have decided to terminate) and continued provision of services constitutes aiding and abetting.³⁸ Moreover, in a situation where the customer company is clearly involved in money laundering, the bank may need to terminate the client relationship to avoid criminal liability under the federal money laundering statutes.³⁹

Thus, the question whether to terminate the customer relationship is fraught with risk both under the Bank Secrecy Act and civil and criminal law.

CONCLUSION

A bank confronted with one of these "red flags" indicating that one of its customers might be operating a Ponzi scheme is faced with so many potential pitfalls that it may be paralyzed into inaction. If it fails to take any action, a plaintiff's attorney could argue that its continued provision of ordinary banking services constitutes aiding and abetting. If it takes action, a plaintiff's attorney could argue that the action demonstrates the bank's knowledge of the underlying fraud. Underlying the bank's decisions is its overriding need to comply with the Bank Secrecy Act and the potential for criminal money-laundering exposure. The ultimate decision whether or not to terminate the customer relationship also must take into account all of these potential risks. It may seem like a bank in this situation is confronted with a classic "damned if you do, damned if you don't" situation. However, as long as a bank complies with its SAR-filing and other Bank Secrecy Act obligations, incorporates "red flags" into its compliance program and does not overly depend on imperfect civil liability defenses, it can appropriately manage the many risks in this area.

NOTES

¹ See *Securities & Exchange Comm'n v. Madoff*, No. 08 Civ. 10791, Complaint, Dkt. No. 1, Tr. 2 (S.D.N.Y. Dec. 11, 2008).

² See *Securities & Exchange Comm'n v. Stanford Int'l Bank Ltd.*, No. 3:09-CV-298-N, Complaint, Dkt. No. 1, Tr. 2 (N.D. Tex. Feb. 17, 2009).

³ Charles Ponzi ran a postage-stamp scheme in the 1920s. See "Ponzi Schemes," April 19, 2001, available at <http://www.sec.gov/answers/ponzi.htm>.

⁴ Senator Arlen Specter also recently introduced a Senate bill which would allow for a private civil action for aiding and abetting violations of the Securities and Exchange Act of 1934 ("Exchange Act"). S. 1551, 111th Cong., 1st Sess., 155 Cong. Rec. S8564 (July 30, 2009). The Supreme Court has interpreted the Exchange Act as not prohibiting aiding and abetting a violation of the Exchange Act. *Central Bank of Denver v. First Interstate Bank of Denver*, 511 U.S. 164 (1994).

⁵ Bank Secrecy Act/Anti-Money Laundering ("BSA/AML") Examination Manual, Appendix F, at F-1 to F-8.

⁶ *Weshnak v. Cosmo*, No. CV 09-1606-ADS-AKT, Class Action Complaint, Dkt. No. 1, Tr. 1-2 (E.D.N.Y. April 17, 2009) (hereinafter *Weshnak*).

⁷ *Collins v. AdSurfDaily, Inc.*, No. CV 09-100-RMC, First Amended Class Action Complaint, Dkt. No. 12, Tr. 4 (D.D.C. April 27, 2009) (hereinafter *Collins*).

⁸ *Metz v. Unizan Bank*, No. CV 05-1510-DCN, Second Amended Class Action Complaint, Dkt. No. 334, Tr. 55-66 (N.D. Ohio. Nov. 11, 2005) (hereinafter *Metz*); *Rotstain v. Trustmark Nat'l Bank*, No. 2009-53845, Plaintiffs' Original Petition, Tr. 3 (Harris County Tex. Aug. 23, 2009) (hereinafter *Rotstain*).

⁹ *Supra Weshnak*, Tr. 2; *Metz*, Tr. 55; *Collins*, Tr. 17-18.

¹⁰ *MLSMK Investments Co. v. JP Morgan Chase & Co.*, No. CV 09-4049, Complaint, Dkt. No. 1, Tr. 12 (S.D.N.Y. April 23, 2009) (hereinafter *MLSMK*).

¹¹ *Supra Rotstain*, Tr. 2-3.

¹² *Supra Weshnak*, Tr. 2.

¹³ *Supra Weshnak*, Tr. 19.

¹⁴ *Amezcuca v. East West Bancorp*, No. CV 09-5168-CAS-JC, Class Action Complaint, Dkt. No. 1, Tr. 12-17 (C.D. Cal. July 16, 2009).

¹⁵ 12 CFR 21.11(c)(4); 31 CFR 103.18(a)(2).

¹⁶ 31 U.S.C. § 5322(a).

¹⁷ See Paul Braverman, "Laundered, Spun and Fined," *The American Lawyer* (June 2, 2005).

¹⁸ 12 CFR 21.21.

¹⁹ *Id.*

²⁰ BSA/AML Examination Manual, Appendix F, at 72-76.

²¹ See *supra* Rotstain; MLSMK.

²² *In re: First Alliance Mortgage Co. v. Lehman Commercial Paper, Inc.*, 471 F.3d 977, 993 (9th Cir. 2006); *Lerner v. Fleet Bank*, 459 F.3d 273, 292 (2d Cir. 2006) (citation omitted).

²³ See *Casey v. U.S. Bank Nat'l Ass'n*, 127 Cal. App. 4th 1138, 1142 (Ct. App. Cal. 2005).

²⁴ *Id.* at 1144 (citations omitted)

²⁵ *Id.* at 1149, 1151-52. See also *Lerner v. Fleet Bank*, 459 F.3d 273, 294 (2d Cir. 2006) (actual knowledge of some impropriety, including multiple overdrafts from an attorney's escrow account and transfers from that account to attorney's personal account, not equivalent to actual knowledge of fraud).

²⁶ *Chance World Trading E.C. v. Heritage Bank of Commerce*, 438 F. Supp. 2d 1081, 1086 (N.D. Cal. 2005) (allegations regarding "atypical banking procedures" including permitting withdrawal with less than requisite number of signatures and unauthorized transfer of funds in violation of internal rules do not allow inference of bank's actual knowledge of client's crime).

²⁷ *Adams v. Fiserv*, 2008 Cal. App. Unpub. LEXIS 6854 (Ct. App. Cal. Aug. 22, 2008) (actual knowledge adequately pled by allegations that the IRA trustees commingled investor and company funds and transferred funds in violation of company's investment offering); *Gonzales v. Lloyds TSB Bank, PLC*, 532 F. Supp. 2d 1200, 1207 (C.D. Cal. 2006) (actual knowledge adequately pled by allegations of the classic hallmarks of a Ponzi scheme including that the defendant bank commingled funds and knew of company's "exceptional returns").

²⁸ 12 CFR 21.11(k); 31 CFR 103.18(e); see also *Union Bank of California, N.A. v. The Superior Court of Alameda County*, 130 Cal. App. 4th 378, 394 (Ct. App. 2005) ("[T]he SAR privilege covers draft SAR's, the SAR's themselves, [] any communication concerning a SAR ... [and] documents prepared by a bank for the purpose of investigating or drafting a possible SAR.") (citation and internal quotation marks omitted).

²⁹ *Neilson v. Union Bank of Cal.*, 290 F. Supp. 2d 1101, 1120-21 (C.D. Cal. 2003) (actual knowledge adequately pled where plaintiffs alleged that the banks "utilized atypical banking procedures" to service Ponzi scheme operator's accounts including banks' failure to properly value plaintiffs' investments, allowing principal to overdraw his account, extending an unsecured line of credit to principal and handling the client accounts as if they were one pool of

assets).

³⁰ *Metz v. Unizan Bank*, No. CV 05-1510-DCN, Report and Recommendation, Dkt. No. 534, Tr. 55-66 (N.D. Ohio. February 8, 2008).

³¹ *Fiol v. Doellstedt*, 50 Cal. App. 4th 1318, 1326 (1996) (“[M]ere failure to act does not constitute the giving of ‘substantial assistance or encouragement’ to the tortfeasor.”); *Renner v. Chase Manhattan Bank, N.A.*, 2000 WL 781081 at *12 (S.D.N.Y. June 16, 2000), *aff’d*, 85 Fed. Appx. 782 (2d Cir. 2004) (“[A]bsent a fiduciary duty, inaction does not constitute substantial assistance.”).

³² *Casey*, 127 Cal. App. 4th at 1149.

³³ *See, e.g., supra, Weshnak*, Tr. 18.

³⁴ *In re: First Alliance Mortgage Co. v. Lehman Commercial Paper, Inc.*, 471 F.3d 977, 995 (9th Cir. 2006); *Casey*, 127 Cal. App. 4th at 1145. This is fortunately not the rule in other jurisdictions. *See, e.g., Mazzaro de Abreu v. Bank of Am. Corp.*, 525 F. Supp. 2d 381, 390 (S.D.N.Y. 2007) (“[T]he mere fact that participants in a fraudulent scheme use accounts at a bank to perpetrate it, without more, does not in and of itself rise to the level of substantial assistance.”) (citation and internal quotation marks omitted).

³⁵ *Lerner*, 459 F.3d at 295 (“[B]anks do have a duty to safeguard trust funds when confronted with clear evidence indicating that those funds are being mishandled.”).

³⁶ 31 U.S.C. § 5318(g)(3).

³⁷ *See, e.g., Ricci v. Key Bancshares of Maine Inc.*, 662 F. Supp. 1138 (D. Me. 1987) (bank’s decision to terminate lending relationship with customer based on erroneous information from the FBI regarding customer’s ties to organized crime resulted in \$15 million verdict in customer’s favor).

³⁸ *See, e.g., supra, Collins*, Tr. 25.

³⁹ 18 U.S.C. §§ 1956, 1957.