Portfolio Media. Inc. | 860 Broadway, 6th Floor | New York, NY 10003 | www.law360.com
Phone: +1 646 783 7100 | Fax: +1 646 783 7161 | customerservice@law360.com

Fraud Victims 'Breaking The Bank'

Law360, New York (February 15, 2011) -- As the architect of the largest Ponzi scheme in recorded history, Bernard Madoff swindled investors out of billions. His actions ruined the lives of countless individuals and, for that, he has been properly punished. The same, however, cannot be said for those that helped Madoff pull off his scam.

Government regulators, some of whom suspected Madoff — but did not stop him — appear to have escaped any significant scrutiny, save for what their own consciences may dictate. The army of individual professionals who helped Madoff manage and operate his schemes may likewise never be called to task for their own infractions. Nevertheless, the bankruptcy trustee, Irving Picard, has made significant progress in collecting huge sums of money for Madoff's victims. And, as new theories of liability emerge, it is possible that even more money will be recovered.

One such theory targets the banks that helped funnel the proceeds of Madoff's crimes. Indeed, banks are becoming a potential piggy bank for defrauded investors to chase — and for good reason. Banks now have the ability to truly identify their customers; to monitor their accounts; and to detect and report suspicious activity to regulators and law enforcement agencies around the world.

In lawsuit after lawsuit, banks are being called to task for ignoring the "red flags" associated with fraud. From the failure to verify sources of money pouring into accounts, to the often blind acceptance of account-holder statements regarding the origin and destination of significant fund transfers between related accounts, these omissions are now forming the basis of a new theory of civil and criminal liability.

To mitigate their risk, banks must return to the principles underlying the Bank Secrecy Act and ensure that their compliance programs sweep broadly enough to include the fraudsters who dominate today's headlines.

The Bank Secrecy Act Gives Banks the Power to Fight Fraud

The Bank Secrecy Act requires that all banks maintain anti-money-laundering compliance programs. These programs consist of internal policies and procedures designed to guard against money laundering and other related crimes like narcotics trafficking and terrorist financing.

Today, the list also includes fraudulent activities like the Ponzi schemes that emerge on a near daily basis. An effective program will include, among other things, KYC or “Know Your Customer” protocols. Through its KYC checks, financial institutions are required to determine the true identity of customers and their businesses.

Under KYC procedures, a bank is supposed to verify the business and the source of monies that come into a business account. KYC further requires banks to monitor their customers’ accounts, and determine whether transactions are legitimate or suspicious. If the latter, banks are required to report the suspicious transaction and close the account. When banks fail in this obligation, they can be subjected to potential liability.

It Happens All the Time

Consider the following scenario, inspired by a recently filed lawsuit in a U.S. district court. A fraudster conceives of a scheme whereby he approaches members of his church and offers to share his investment advice. His goal, he claims, is to help his fellow churchgoers become wealthy in their own right so that they too can give back to the church and their community.

In order to entice potential investors, the fraudster becomes very active in church-related groups. The more people he meets, the bigger his potential pool of investors. At each meeting, he produces various printed materials, touting above-normal returns in a very short period of time. As he is fond of telling anyone who will listen, “Your money will be invested for so little time that you won’t even know it's missing. And, when you get it back, your investment will have doubled in size!” Once he sees that a person is interested, the fraudster turns up the pressure, urging the potential investor to move quickly or risk missing out on the opportunity of a lifetime.

To further create a false sense of security with respect to potential investments, the fraudster creates a “management and oversight agency” which will collect investor monies and monitor their investments. The fraudster tells potential investors that this is an independent company that supervises the investment products he is selling. If the agency at any point determines that there is a risk of loss, it will require that he refund the principle investment. For good measure, the fraudster adds that the agency provides investors with insurance that will not only protect their principal amount, but also provide interest on their investment. Either way, then, investors cannot lose.

Once sold on the scheme, investors contribute a minimum of $1,000. Investors would not be able to recover their money for at least 90 days. At the end of that period, each investor would purportedly receive their principal and profits, minus a significant commission to be paid to a company ultimately owned by the fraudster.

These returns, of course, were not legitimate. The monies returned were never actually the product of wise investing, but additional funds collected from other hapless investors. To perpetuate the scheme, the fraudster would generate fake account statements, which showed a significant return on the initial investment.

As money poured in, the fraudster would take the funds held by the sham management and oversight agency and transfer them to accounts owned by his own financial services company. In this way, the fraudster eventually transferred millions of dollars into his own personal bank accounts from which he made significant cash withdrawals.

Initially, the fraudster maintained all of his related accounts at one local bank. However, when that bank indicated that it would be closing his accounts due to suspicious activity, the fraudster searched for a new "friendlier" bank. He quickly found one.

A large bank with branches throughout the U.S. offered the fraudster its services. Notably, this bank overlooked all of the red flags cited by the previous financial institution and allowed the fraudster to open several accounts despite obvious suspicious activity. The bank accepted the fraudster's vague statement that he was moving his accounts because he did not believe his prior bank was "business friendly."

The bank accepted this representation and never made any effort to contact the prior bank. Had it done so, it would have learned the accounts were closed because the transactions being conducted were not consistent with a legitimate business. Indeed, had the new bank bothered to conduct even the most rudimentary of searches on publicly available databases, it would have discovered that its new customer had a record of engaging in improper (even criminal) business practices.

Shortly after the fraudster opened his new accounts, several additional accounts were opened by the management and oversight agency that collected investor funds. These additional accounts brought several million dollars into the bank, most of which were later transferred into the fraudster's corporate accounts.

In the weeks following the opening of these new accounts, the fraudster withdrew more than $300,000. At no point in time did bank representatives make any inquiries regarding the withdrawals. To the contrary, the bank made the fraudster's life easier by implementing a procedure where he, or one of his agents, could pick up large amounts of cash from a branch's drive-thru window.

Had the bank properly applied its KYC protocols, it would have discovered that all of the funds flowing into the fraudster's corporate accounts came from the related management and oversight agency accounts. In fact, this was the only source of income into the fraudster's corporate accounts.

Of course, the fact that the bank ignored these suspicious activities did not mean that it did not document them. Internal documents — obtained by lawyers for defrauded investors — later revealed that the bank was concerned that some of the accounts related to the fraudster were engaging in suspicious activities. And the bank did freeze one of the accounts at issue.

However, the bank unfroze the account a few days later after reviewing a business plan that purportedly legitimated the suspicious activity in question. Not only did the business plan not make any sense, it was flatly contradicted by the transactions the bank monitored through the fraudster's accounts on a daily basis.

By the time the bank took action to close all of the accounts, several million dollars had already passed into the fraudster's hands. When the Ponzi scheme unraveled, a receiver was named on behalf of the fraudster's corporate entities. The receiver quickly identified the bank and filed suit seeking damages for aiding and abetting a breach of fiduciary duty, aiding and abetting conversion, and negligence.

Whether the bank prevails in this action is ultimately a secondary question. In defending against these lawsuits, banks must be conscious of the potential impact that civil and criminal actions can have on the bank's ability to continue doing business.

Mitigating Risk

The reality is that banks cannot eliminate risk. If a plaintiff's lawyer decides that a particular institution is liable (or can be forced into a quick settlement), the lawsuit will likely come. Thus, the key question here is what can banks do to mitigate their legal risk? In discussing the term "legal risk," it is important to note that financial institutions can face both civil and criminal liability. To survive, banks must learn to manage these risks effectively.

Violations of the Bank Secrecy Act, for example, can carry a criminal penalty that includes imprisonment for individual bank officers and employees, as well as hefty fines. In addition, banks may also face civil liability as discussed in the example above.

Even more complicated is the fact that lawyers in a civil action on behalf of defrauded investors may point to a bank's compliance or noncompliance with the Bank Secrecy Act's reporting requirements as evidence of liability. The filing of a suspicious activity report (SAR) may keep a financial institution from facing criminal liability, but provide a plaintiff's lawyers with ammunition to go after a bank for its alleged "knowledge" of the fraud.

The failure to file an SAR, in turn, may be used as evidence of the bank's complicity in the fraud itself. Some may call this a Hobson's choice, where financial institutions will be caught in the cross-hairs regardless of what they do. That view, however, is somewhat shortsighted.

In the example discussed above, the fraudster's bank clearly committed a violation of the Bank Secrecy Act. By failing to report the suspicious transactions its own internal documents confirmed were detected, the bank exposed itself to potential criminal penalties.

Indeed, if it were established that the bank knowingly failed to report the suspicious activity — and the facts as recounted above strongly suggest that the bank knew exactly what was happening — the penalties could be crippling. Criminal prosecution carries grave consequences. A bank's ability to continue operating could be seriously impacted by arrests, indictments and guilty pleas which carry stiff financial penalties.

Moreover, the negative publicity stemming from a criminal investigation may undermine investor confidence, to say nothing of those who maintain accounts at the particular bank. Thus, banks should be focused, first and foremost, on complying with the Bank Secrecy Act.

If a financial institution is sued by a group of defrauded investors or other plaintiffs, it will have defenses. Courts around the U.S. have recognized defenses based on a lack of knowledge and the absence of a fiduciary duty. However, these are not perfect defenses. Questions of knowledge are usually resolved by a jury, which means that a bank may find itself locked in prolonged litigation, which culminates in a risky trial.

Once a case goes to the jury, a bank will lose its ability to control the outcome of the case. Other defenses, including those claiming a lack of fiduciary duty, may only complicate matters. A bank claiming that it owes no duty to noncustomers cannot simply overlook suspicious activities. If a transaction raises a red flag, the Bank Secrecy Act compels the filing of a SAR. The failure to do so could lead to criminal penalties.

Litigation against financial institutions on behalf of defrauded investors is still in its infancy. As courts across the U.S. consider individual lawsuits and make decisions concerning viable theories of relief and available defenses, the legal landscape will become clearer. This, in turn, will allow financial institutions, their officers and their attorneys to map out even more effective risk-mitigating strategies.

For now, the best advice for financial institutions is to ensure that they are complying with the Bank Secrecy Act, that their internal compliance programs are updated, and that officers, directors and front-line employees are properly trained in the potential red flags associated with fraud.

--By Michael Diaz Jr. and Carlos F. Gonzalez, Diaz Reus & Targ LLP

Michael Diaz (mdiaz@diazreus.com) is the founding partner of Diaz Reus & Targ LLP and managing partner in the firm's Miami office. He concentrates on international and complex commercial litigation, regulatory matters, and internal investigations and white collar criminal defense. Carlos Gonzalez (cgonzalez@diazreus.com) is a partner in the firm's Miami office, focusing on litigation and appeals before state and federal courts, with a focus on international, commercial, and criminal matters. Both Diaz and Gonzalez are Certified Anti-Money Laundering Specialists.