



WHAT BANKS SHOULD BE DOING TO PROTECT THEMSELVES

Financial institutions can be held liable for not guarding against fraudulent activity by their customers, but compliance with the Bank Secrecy Act can help lower the risk.

FROM FRAUDSTERS STEALING FROM UNSUSPECTING INVESTORS

MICHAEL DIAZ, JR., CARLOS F. GONZALEZ, MARGARET T. PEREZ, AND XINGJIAN ZHAO

Bernard Madoff's Ponzi scheme swindled unsuspecting investors out of billions of dollars of their hard-earned cash. As the mastermind behind what is possibly history's largest and most sophisticated act of financial fraud, Madoff has ruined countless lives. While Madoff has been punished for his acts, those who assisted him with his fraud have not. Government regulators and overseers who turned a blind eye to Madoff's deception have

escaped liability unscathed. The army of professionals who helped Madoff manage and operate his schemes may never be held legally accountable for their assistance. Nevertheless, the trustee, Irving Picard, is making significant progress in collecting money for the victims of Madoff's scheme. And, as new theories of liability emerge, it is possible that even more money will be recovered for Madoff's victims.

One theory of liability focuses on the banks that helped funnel the proceeds of Madoff's Ponzi scheme. Indeed, banks are becoming potential treasure troves for defrauded investors trying to salvage what they have lost—and for good reason. Banks are now capable of detecting

MICHAEL DIAZ, JR. is the managing partner of Diaz, Reus & Targ LLP in the firm's Miami office and a former assistant state attorney for Janet Reno. CARLOS F. GONZALEZ is a partner with the firm in the Miami office. MARGARET T. PEREZ is an associate with the firm in Miami and XINGJIAN ZHAO is an associate with the firm in Shanghai.

their customers' true identities, actively monitoring their accounts in real time, and accurately detecting, pinpointing, and reporting suspicious activity to regulatory authorities and law enforcement agencies around the world. Across the country, in case after case, banks are being called to task for having ignored the "red flags" associated with fraud. From the failure to verify the sources of money pouring into previously illiquid accounts to the often blind acceptance of customer statements regarding the origin and destination of hefty fund transfers between

LOCAL CREDIT UNIONS AND SAVINGS AND LOANS ARE JUST AS LIKELY TO BE SUED AS THEIR GLOBAL COUNTERPARTS.

related accounts, these unfortunate omissions are now forming the basis of a new theory of civil and criminal liability toward

which society, as well as courts, can be highly sympathetic. To mitigate their risk, banks must steadfastly adhere to the principles underlying the Bank Secrecy Act. They must ensure that their compliance programs cast a wide enough net so that fraudsters who dominate today's headlines can be caught before inflicting significant damage.

The Bank Secrecy Act gives banks the power to fight fraud

Under the Bank Secrecy Act, all banks must maintain anti-money laundering compliance programs. These programs consist of internal policies and procedures designed to safeguard against abuses such as money laundering and other crimes, including tax evasion, narcotics trafficking, and terrorist financing. Today, this watch list also includes fraudulent activities like Ponzi schemes. An effective internal compliance program will include, among other things, "Know Your Customer" (KYC) protocols. Through their KYC checks, financial institutions are required to determine the true nature and identity of customers and their businesses. KYC procedures require banks to verify the business and the source of funds that come into a business account. They further require banks to actively monitor their customers' accounts and deter-

mine the legitimacy of transactions to and from those accounts. If a transaction is deemed suspicious, banks are required to report the transaction and close the account. When banks fail in this obligation, they may be accused of negligence.

Big banks are feeling the heat

Picard's recent high-profile lawsuits against JPMorgan Chase and HSBC represent just a handful of many such lawsuits. These suits target banks for failing to live up to the Bank Secrecy Act's implicit obligation for them to serve as the financial regulators' direct confidants—the first line of defense against all types of financial fraud. In the case against JPMorgan, Picard is suing the bank for \$1 billion in fees and an additional \$5.4 billion in damages, accusing it of "aiding and abetting Madoff's fraud" during its "decades-long role" as Madoff's primary banker.¹ Separately, Picard is suing HSBC for 24 counts of financial fraud and other misconduct and seeks to recover from it "at least \$9 billion" in addition to unspecified punitive damages. In this suit, Picard claims that HSBC, while marketing Madoff's funds overseas, was "willfully and deliberately blind to the fraud."²

Smaller banks are also susceptible

Local credit unions and savings and loans are just as likely to be sued as their global counterparts. Notably, there is a pending class action lawsuit against TD Bank and Gibraltar Private Bank of Coral Gables, Florida. These small banks are being accused of violating their own compliance procedures, "blindly authorizing" a number of suspicious wire transfers, and disregarding "apparent fraud warning signs" associated with the accounts of Scott Rothstein, a disgraced Fort Lauderdale attorney who recently pleaded guilty for defrauding investors in a \$1.2 billion Ponzi scheme.³ Smaller doesn't mean safer.

It happens all the time

Consider the following scenario, inspired by one of many recently filed lawsuits in

THE MONIES RETURNED ARE NOT GAINS ON INVESTMENTS, BUT RATHER ADDITIONAL FUNDS COLLECTED FROM OTHER HAPLESS INVESTORS.

a federal district court. A fraudster conceives of a scheme where he approaches members of his church and offers to share his investment advice. His goal, he claims, is to help members of his congregation become wealthy in their own right, so that they, too, can give back to the church and their community. In order to attract investors, the fraudster becomes very active in pursuing extra-curricular activities, such as joining church groups and expanding his social circle. As he meets more people, he grows his potential pool of investors. At each meeting, he produces glossy brochures, touting above-normal returns in a very short period of time. During his pitch, he always tells them, “Your money will be invested for so little time that you won’t even know it’s missing. And, when you get it back, you’ll have twice as much!” Once he recognizes that someone has taken the bait, the fraudster begins pressuring the potential investor, urging him to move quickly or risk missing out on a once in a lifetime opportunity.

As another part of the elaborate scheme, and in order to create a false sense of security, the fraudster creates a “management and oversight agency” to hold the investors’ monies and monitor their investments. He informs the potential investors that the management and oversight agency is an independent entity that will supervise the investment products he is selling. He claims that if the agency determines that there is a risk of loss, it will require that he refund the principle investment to the investor. As added comfort, the fraudster says that the agency provides insurance that protects both the principal amount and also the interest on their investment. Either way, it’s a win-win situation for investors—or so the fraudster claims.

Once the investors are convinced, they are required to contribute a minimum of \$1,000, which is not recoverable for at least 90 days. At the end of the 90 day period, the investor is to receive his principal and profits, minus a significant commission to be paid to a company ultimately owned by the fraudster. This, however, does not occur. The monies returned

are not gains on investments, but rather additional funds collected from other hapless investors. As another part of the elaborate scheme, the fraudster generates false account statements purporting to show the significant return on the initial investment.

As the fraudster attracts more investors, he takes the money that was held by the so-called independent management and oversight agency and transfers the funds to accounts held by his own financial services company. During the course of the scam, the fraudster transfers millions of dollars into his own personal bank accounts and subsequently makes significant cash withdrawals. At the beginning of the scheme, the fraudster maintains the accounts for the agency and his own financial services company at the same local financial institution. However, once his accounts are flagged for suspicious activity and he is notified that the bank will be closing his accounts due to that activity, the fraudster seeks another bank that will be more accommodating.

This “friendlier” bank is, in fact, a large bank with branches throughout the United States. Ignoring the red flags raised by the previous bank, this new financial institution offers the fraudster carte blanche. The new bank permits the fraudster to open several accounts despite obvious suspicious activity. The fraudster tells the new bank that he is moving his accounts from the local bank because he believes it is not “business friendly.” The new bank makes no effort to contact the fraudster’s former bank. If the bank actually did its due diligence, it would discover that the prior bank closed the accounts because the transactions being conducted were not consistent with a legitimate business. In fact, if the larger bank engaged in a cursory search of publicly available databases, it would discover that its new customer has an extensive record of engaging in deceptive—and even criminal—business practices. None of this is done.

Once the fraudster opens his new accounts for the financial services company at the new bank, he then opens accounts for the management and over-

sight agency to collect investor funds. In a short period of time, millions of dollars are deposited into the agency's accounts, most of which are subsequently transferred into the fraudster's corporate accounts. The fraudster, in just a few short weeks, withdraws more than \$300,000. Despite this highly irregular activity, the financial institution never makes any inquiries regarding the suspicious withdrawals. To the contrary, the bank actually makes the fraudster's life easier by implementing a procedure where he, or one of his agents, never needs to set foot into a bank branch; instead, they can pick up large amounts of cash from a branch's drive-thru window. If the bank properly applied its KYC protocols, it would quickly learn that all of the funds flowing into the fraudster's corporate accounts came from the related management and oversight agency accounts. These funds are, in fact, the only source of income flowing into the accounts of the financial services company.

Even though the bank does not implement its KYC procedures and does not flag these transactions as they occur, they still document the activity. Lawyers for the defrauded investors obtain internal bank documents revealing the bank's concern that some of the accounts related to the fraudster contain proceeds stemming from fraudulent activity. The lawyers learn, after reviewing the documents, that the bank did freeze one of the accounts at issue. However, the bank then unfroze the account a few days later, after the fraudster provided the bank with a business plan that purportedly legitimized the suspicious activity in question. This business plan is nonsensical and was plainly contradicted by the transactions the bank monitored through the fraudster's accounts on a daily basis. By the time the bank takes action to close all of the fraudster's accounts, the fraudster has already transferred millions of dollars from the agency's accounts to the financial services company's accounts. Once the Ponzi scheme comes to public light, a receiver is named on behalf of the fraudster's corporate entities. The receiver moves quickly and identifies the bank. The receiver subsequently files suit against the bank, seeking dam-

ages for aiding and abetting a breach of fiduciary duty, aiding and abetting conversion, and negligence.

Whether the bank prevails in this action is not the most important issue. Rather, 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

In reality, banks cannot eliminate risk; they can only reduce it. If a plaintiff's lawyer decides that a given institution can be held liable (or can be forced into a quick settlement), a lawsuit will likely be filed. 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 not only civil liability but criminal liability as well. To shelter themselves, banks must learn how to effectively manage these risks and become more risk averse.

Violations of the Bank Secrecy Act, for example, can subject individual bank officers and employees to criminal penalties, including imprisonment and hefty fines. In addition, banks may also face civil liability, as is shown in the example above. Even more unsettling is the fact that lawyers in a civil action on behalf of defrauded investors may point to a bank's compliance or non-compliance with the Bank Secrecy Act's reporting requirements as evidence of liability. Filing a Suspicious Activity Report (SAR), for example, may keep a financial institution from facing criminal liability, but imputing "knowledge" of the customer's fraudulent activities provides lawyers with legal ammunition to go after a bank in court. The failure to file a SAR, on the other hand, may be used as direct 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 our case study, the fraudster's bank clearly violated key provisions of the Bank Secrecy Act. By failing to report



IN REALITY, BANKS CANNOT ELIMINATE RISK; THEY CAN ONLY REDUCE IT.

the suspicious transactions that the bank's own internal documents confirmed were detected, the bank, as well as its officers and employees, exposed itself to potential criminal liability. Indeed, if it were established that the bank knowingly failed to report the customer's suspicious activity—and the facts as recounted above strongly suggest that the bank knew exactly what was going on—the penalties could be crippling. The consequences of a criminal prosecution are grave. The effect of arrests, indictments, and guilty pleas, which carry stiff financial penalties, can jeopardize a bank's ability to continue operating. Moreover, the negative publicity stemming from a criminal investigation will severely undermine investor confidence, to say nothing of those existing customers who maintain accounts at the particular bank under investigation. Thus, a bank's first and foremost focus should be complying with the Bank Secrecy Act.

That said, if a group of defrauded investors or other plaintiffs sue a financial institution, the bank will have defenses. Courts around the U.S. have recognized various defenses based on a lack of knowledge and the absence of a fiduciary duty. However, these defenses are far from perfect. Juries, not judges, are usually charged with resolving questions of knowledge, which means that a bank may find itself locked in protracted litigation culminating in a risky and costly trial. Once the case goes to the jury, a bank loses all ability to control its outcome. Other defenses, including

a lack of fiduciary duty, may only further complicate matters. A bank claiming the absence of a fiduciary duty to non-customers cannot simply overlook its own customers' suspicious activities. If a transaction raises a red flag, the Bank Secrecy Act compels the filing of a SAR, regardless of the circumstances surrounding the transfer. The failure to do so could lead to criminal penalties.

Currently, litigation against financial institutions on behalf of defrauded investors is still at a budding stage. As courts across the U.S. hear specific lawsuits and issue rulings concerning various theories of relief and available defenses, the contours of 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 all aspects of the Bank Secrecy Act, that their internal compliance programs are up to date, and that their officers, directors, and frontline employees are properly trained in identifying the red flags associated with fraud. ■

NOTES

¹Complaint, *Picard v. JPMorgan Chase & Co.*, No. 10-AP-4932 (Bankr. S.D.N.Y. 2011).

²Press Release of Irving H. Picard, "Trustee for Liquidation of Madoff Investment Securities Seeks \$9 Billion in Recoveries, and Additional Damages at Trial, From HSBC, Related Entities, Feeder Funds in Madoff Ponzi Scheme" (Dec. 5, 2010).

³Complaint, *Razorback Funding, LLC, et al. v. Scott W. Rothstein, et al.*, No. 09-062943 (07) (Fla. 17th Cir. Ct. 2009).