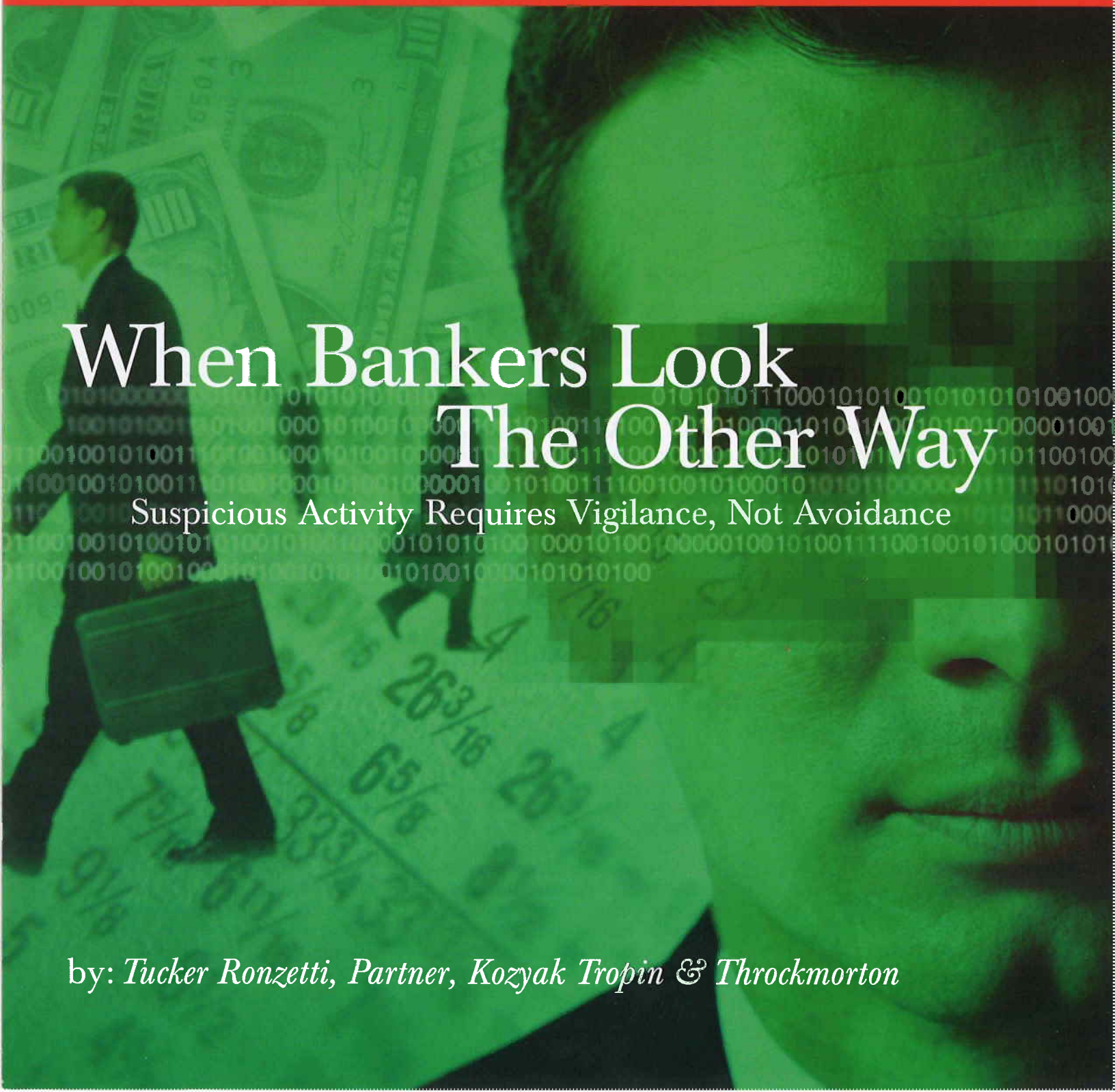
AN ARTICLE FROM

Business Law Today

Volume 14, Number 5



When Bankers Look The Other Way

Suspicious Activity Requires Vigilance, Not Avoidance

by: *Tucker Ronzetti, Partner, Kozyak Tropin & Throckmorton*

When Bankers Look The Other Way

Suspicious Activity Requires Vigilance, Not Avoidance

by: *Tucker Ronzetti, Partner, Kozyak Tropin & Throckmorton*

Legend has it that when the notorious thief "Slick" Willie Sutton was asked why he robs banks, he answered, "Because that is where the money is." But Slick Willie, like most thieves who rob at the point of a gun, spent more of his lifetime in a jail than out of one. In today's world, stealing is easier and safer without a gun. The old-fashioned bank heist has become more rare. A bank is more likely to be used by a sophisticated thief as an instrument to steal from others, through money laundering and financial fraud.

Banks process millions of transactions every day. The vast majority of these are ordinary and legitimate, but many are not. Every day, hundreds of millions of dollars of illegal transactions run through the banking system, ranging from a simple forged check to entire systems of money laundering and financial fraud committed through wire transfers.

Banks, Be Wary

Federal law has long required banks to be wary of such illegal conduct. Enacted in 1970, the Bank Secrecy Act began the conscription of bank employees into the war against money laundering and other forms of financial crimes. That law led to the adoption of "know your customer" policies by financial institutions throughout the country. Such policies promote banks' understanding of the customer's identity, the purpose of the customer's accounts, and the types of transactions the customer is expected to have, in order to combat the illegal use of financial services.

Subsequent regulations have required banks to report suspicious activity, including any potentially criminal conduct, to a centralized federal authority, the Treasury Department's Financial Crimes Enforcement Network, or "FinCEN." Most recently, the USA PATRIOT Act has led to additional requirements for banks to identify and verify the identity of customers opening new accounts. For further background on these regulations see FinCEN's Web site, www.fincen.gov.

Although these banking regulations are in tension with the traditional and legal requirements of customer confidentiality, for the most part they have not led to substantial liability. Beneficent legislation has helped. Recognizing potential lawsuits from reporting requirements, Congress provided a "safe harbor" provision so that banks properly reporting suspicious activity cannot be held liable by the customer involved. See 31 U.S.C. § 5318(g)(3).

> ***"A party who knows of wrongdoing and yet helps the wrongdoer can be as liable as the wrongdoer himself."***

Banks Risk Liability

A bank can, however, risk liability under the common law for failing to report illegal conduct, where that failure implicates the bank in fraudulent activity. And the risks suffered by banks extend to one degree or another to every company involved in financial services.

Across the country, fraudulent schemes abound. See some described at the nonprofit National Fraud Information Center's Web site, www.fraud.org. In many of these schemes, criminals defraud investors with promises of healthy returns on their money, when in reality the "investments"are nothing but a sham.

A fraudulent investment scheme of any substantial size requires the services of a financial institution to continue. Banks are needed to gather the money from the victim "investors" and provide them with "returns" which, in reality, are nothing more than a portion of the investor's own money. Most important for the criminals, financial institutions are needed to help steal the money by laundering it through other accounts, covering their trails and then hiding the money in overseas bank haven countries or their own pockets. When, despite knowledge of such fraudulent conduct, banks provide their assistance to the scheme, liability results.

Aiding and Abetting

Banks used in fraudulent schemes risk liability based on common law aiding and abetting. Under an aiding and abetting theory, a party who knows of wrongdoing and yet helps the wrongdoer can be as liable as the wrongdoer himself. As stated in the Restatement (Second) of Torts § 876: "For harm resulting to a third person from the tortious conduct of another, one is subject to liability if he...knows that the other's conduct constitutes a breach of duty and gives substantial assistance or encouragement to the other so to conduct himself."

Courts applying aiding and abetting principles in the financial services context focus on two elements, "knowledge" and "substantial assistance." The term "knowledge" in aiding and abetting means "general awareness that one's role was part of an overall activity that is improper." Woodward v. Metro Bank of Dallas, 522 F.2d 84, 95 (5th Cir. 1975). "Substantial assistance" also entails a degree of knowledge, which varies depending on the relationship of the parties and the type of transactions at issue. At one end of the spectrum, where the plaintiff and the bank have no special relationship and the transactions at issue were ordinary, the highest level of knowledge — scienter or "conscious intent" to aid the fraud — must be shown. On the other hand, where the bank has a special relationship with the plaintiff, the bank may be liable for inaction in failing to prevent the fraud, and knowledge may be inferred from business transactions that are atypical or lack business justification.

Based on these principles, aiding and abetting liability does not apply when a bank serves as nothing more than a passive mechanism for illegal transactions. The bank has little risk of liability where it serves as a mechanical clearinghouse alone, because the bank cannot have "known" of the wrongdoing. Where, however, the bank

becomes substantially involved in the transactions — oftentimes through personal bankers trying to accommodate wealthy clientele — the bank's risk of liability multiplies. This may be the case where the bank becomes a tool of a fraudulent financial scheme.

Bank Becomes Tool Of Fraud

A fraudulent scheme called Cyprus Funds illustrates the typical situation. Purportedly a mutual fund, Cyprus Funds was run by a wealthy South American named Eric Bartoli. Cyprus Funds was supposed to have investments in conservative securities as well as certain Latin American holdings. Bartoli led a lavish lifestyle with a mansion and expensive cars, and explained that Cyprus Funds' success came from conservative investments in U.S. and Latin American companies.

In reality, Cyprus Funds was a "Ponzi" scheme — the type of fraud where investors are repaid their own money so that the scheme appears to be a successful investment and more investors can be hoodwinked. This form of scheme originated with Charles Ponzi, who defrauded millions in the 1920s by falsely claiming he could sell international postal coupons at 100 percent profit. Ponzi financed his purported business through promissory notes, which he always readily repaid.

Participating In A Sham

Ponzi's business, in actuality, was a sham. Rather than paying money from profits, Ponzi was paying investors their own money back. As Chief Justice Taft explained, Ponzi "was always insolvent, and became daily more so, the more his business succeeded. He made no investments of any kind, so that all the money he had at any time was solely the result of loans by his dupes." Cunningham v. Brown, 265 U.S. 1, 8 (1924). There have been hundreds of similar schemes. While no official statistics are available, a word search on a federal case database yielded more than 1,000 references to Ponzi.

In the Cyprus Funds Ponzi scheme, hundreds of investors from Ohio to Latin America contributed their money. Eric Bartoli and the other insiders to the scheme needed the assistance of financial institutions to perpetrate and sustain such a fraud. Banking services were required to gather the investors' money, provide the money back to them, and launder the money through wire transfers.

Beyond providing ordinary financial services, the bankers went several steps further. For instance, one banker attended a solicitation trip in Latin America with Bartoli. Evidence revealed that in the course of several solicitations, Bartoli would indicate that the bank at issue was the "custodian of the fund" for Cyprus Funds, when that was simply false.

Bank's Knowledge

Also, evidence showed that through personal banking services, the bank specifically approved a number of suspicious wires conducted by Bartoli, establishing the bank's knowledge of Bartoli's improper transactions. Despite this and other evidence of the bank's knowledge, the Cyprus Funds scheme continued, using the bank to draw more investor money in and to transfer and steal their money.

Throughout all of this, no bank involved with Cyprus Funds ever filed a suspicious activity report, much less shut down the accounts used in the scheme. The result was that investors continued pouring money into the fraudulent fund until the Securities and Exchange Commission finally stepped in. Cyprus Funds and related companies were placed into receivership.

Soon the Cyprus Funds investors learned that Bartoli and others had stolen more than $35 million. Much of the money was stolen through sham companies, which received wire transfers from the Cyprus Funds' bank accounts, either directly or laundered through other entities' accounts. The scam defrauded more than 530 investors, many elderly retirees, leaving lives and families in ruin.

In a lawsuit that followed, the investors claimed that a Miami bank branch aided and abetted the Cyprus Funds Ponzi scheme. Relying on expert testimony establishing that the bank had engaged in "atypical" activity, the district court denied the bank's motion for summary judgment and allowed the case to proceed to trial. Smith v. First Union National Bank, 2002 WL 31056104 (S.D. Fla. Aug. 23, 2002).

In Smith, the court acknowledged that evidence of aiding and abetting is typically circumstantial — those who help a Ponzi scheme rarely confess — and so proof may consist of atypical conduct indicating knowledge of and assistance in the wrongdoing. Evidence of multiple wire transfers performed without apparent legitimate business reasons, wires to bank haven countries typically involved in money laundering, unusual correspondence, loans and a business trip assisting Bartoli, and a statement by the bank's personal representative "acknowledging a degree of malfeasance," all while failing to report suspicious activity as the law requires, tended to show the bank aided and abetted the Cyprus Funds fraud.

Bank's Culpability

Throughout the analysis, "know your customer" and suspicious reporting requirements tended to show the bank's culpability. Because the law and the bank's own policies required the bank to know the nature of Cyprus Funds and its transactions, and to report any suspicions of criminal conduct, it was difficult for the bank to deny such knowledge.

The Smith case was also permitted to proceed as a class action on behalf of the hundreds of investors who had been defrauded. Aiding and abetting liability lends itself to class prosecution in the Ponzi scheme setting, because assistance to the scheme usually affects the entire class of investors. In the midst of trial, the Smith case finally ended when the bank settled for $5 million.

Tucker Ronzetti is a partner in the Miami-based firm Kozyak Tropin & Throckmorton and a key member of the firm's litigation practice. Prior to joining Kozyak Tropin & Throckmorton, Mr. Ronzetti clerked for Judge Edward B. Davis of the Southern District Court of Florida and served as an assistant county attorney for Miami-Dade County. He is an adjunct professor at the University of Miami School of Law, where he earned his law degree and served as editor of the Law Review. He earned his bachelor's degree in economics from Duke University.

Another Ponzi scheme that led to financial institutions' liability was called InverWorld, operated out of San Antonio, Texas. InverWorld purported to provide banking and brokerage services to Latin American investors who sought the security of U.S. investments. In reality, the company was a Ponzi scheme, investing only a portion of the funds while laundering and stealing the bulk.

Another Bank-Assisted Fraud

Such a financial fraud, like the Cyprus Funds Ponzi scheme, required the assistance of banks. InverWorld had successive relationships with banks that assisted in wiring billions in funds that the company circulated in order to launder and conceal its ill-gotten gains.

Two successive banks involved in InverWorld's dealings learned of several red flags that, with adequate investigation, revealed its improprieties. The Internal Revenue Service levied millions in fines on one of InverWorld's related companies. A company called Aeromexico sued and claimed InverWorld was involved with money laundering — a claim publicized in a Wall Street Journal article. At the same time, millions were circulated through circular transactions.

Despite these and other causes for investigation, InverWorld's banks continued to provide financial services, going so far as to provide the company itself the means to perform its own wires. Internal documents indicated that the chief concern of the banks was not InverWorld's fraud, but credit risk. Bank officers apparently reasoned that, as long as only cash transactions were involved, and not a credit, the bank need not be concerned with InverWorld's conduct.

Fraud Led To Litigation

No bank filed a suspicious activity report against InverWorld, and the fraud continued until finally the government stepped in. As with Cyprus Funds, the InverWorld fraud led to litigation. One case has settled, and the other remains pending.

Frauds like Cyprus Funds and InverWorld hurt investors and the reputations — and often the wallets — of financial institutions. At the same time, Cyprus Funds teaches valuable lessons for banks and other financial services companies to avoid liability in the future, or alternatively for defrauded investors to seek a recovery from financial institutions that ignore those lessons.

First, merely adopting "know your customer" rules and suspicious activity reporting requirements will do little to prevent liability. To the contrary, incorporating such rules and requirements into bank policy manuals will lead to a greater risk of liability where those manuals are ignored in practice. A defrauded investor would rightfully ask, why did the bank ignore its own well-settled policies?

Of course, such policies are necessary, and examiners require them. But beyond maintaining the policies, banks need to train staff to abide by the policies and to reward appropriate conduct through employees' paychecks and bonuses.

Report Suspicious Activity

Most important, bankers must promptly report any suspicious activity to the appropriate authorities. Beyond that, if after investigation any doubt exists about the customer, the bank should shut down all the accounts of those involved in the suspicious conduct. To achieve this, bank management should institute compensation policies that reward the prudent handling of such accounts. Banks that exclusively reward fee-generating activity help establish the motive for aiding and abetting misconduct.

Without leadership, it is difficult for bank account representatives to resist the temptation to "cut the red tape" to satisfy wealthy account holders. All too often bank employees will ignore accounts that present little traditional credit risk to the bank. Such temptations must be put in check, and bankers must not only remain vigilant, but also consider themselves an integral part of the financial security of the bank and those who could be defrauded through the bank, in order to avoid risks in litigation and preserve their reputations.

Bank Must Pay

When banks and other financial services companies fail to maintain vigilance and instead willfully ignore criminality, investors and consumers who suffer through fraudulent schemes will turn to those banks for compensation. Faced with the ruined lives of defrauded investors on one hand, and on the other, a sophisticated financial institution bound legally to know the customer and report suspicious conduct, a jury may well determine that the bank must pay for aiding and abetting misconduct. ■

Checklist For Banks

- *Maintain and regularly train employees in "know your customer" and suspicious reporting standards.*
- *Establish and enforce policies to close suspicious accounts.*
- *Provide employee incentives for monitoring and reporting.*
- *Scrutinize questionable cash transactions as carefully as credit transactions.*

KOZYAK • TROPIN
THROCKMORTON
ATTORNEYS AT LAW

2525 Ponce de Leon, 9th Floor
Miami, Florida 33134

Tel: (305) 372-1800
Fax: (305) 372-3508
www.kttlaw.com

This article, "When Bankers Look The Other Way," appeared in **Business Law Today**, Volume 14, Number 5, May/June 2005.