there is a reason that RICO is a four-letter word

by Richik Sarkar

Almost immediately after society developed currency, people started using banks to safeguard their money. While the banking system has changed through the years—with banks and other types of financial institutions offering more products and services than ever before—its primary function remains the same. Banks put the money of others to work by taking their customers' deposits and investments and lending that money to others so they can buy homes and cars, pay for their education and put their children through college, establish and expand businesses and many other productive purposes.

Not surprisingly, once banks became depositories of money, people started to rob them. Willie Sutton established this fact when he explained that he robbed banks "...because that is where the money is." Today, however, the progeny of Mr. Sutton are not the only ones robbing banks. **Banks are now victimized by being named in lawsuits based upon the bad acts of their customers even though they have no involvement with the acts beyond an arm's length business relationship.** The people and attorneys who bring such claims seem to prove the observation of the noted philosopher, Don Henley, drummer for the Eagles, who noted that "a man with a briefcase can steal more money than any man with a gun."

In rare instances it can be claimed that banks and/or their employees were actually involved in nefarious acts. More often than should be tolerated, banks are simply included in lawsuits because they are deep pockets. These improper deep pocket actions often take two forms: claims under the Racketeer Influenced and Corrupt Organizations Act (RICO) and common law aiding and abetting claims. **The reason these claims are used, often without any real basis, is simple: The first allows for treble damages and the second can give rise to punitive damages; terms which cause clients and attorneys great worry.** Defending against such claims can be complicated; however, when a bank's only connection to a situation is the fact that a wrongdoer simply maintained an account with or obtained a loan from a bank or financial institution, banks should not be involved.

The original purpose of RICO was to combat the infiltration of legitimate businesses by organized crime and "to seek the eradication of organized crime in the United States." **Despite the stated goal, RICO is, improperly, invoked to attempt to hold banks liable for the actions of their account holders who may have defrauded people and stolen money.** When the victims of the fraud discover the wrongdoer has no assets, they begin the search for other deep pockets. Banks are often the most convenient target because the bad guy had an account at a local branch and, of course, "that is where the money is" or, more realistically, was.

Civil RICO cases are "the litigation equivalent of a thermonuclear device" and the mere assertion of a RICO claim has "inevitable stigmatizing effect on those named as defendants;" because of this, many courts "strive to flush out frivolous RICO allegations at an early stage of the litigation." *Dubai Islamic Bank v. Citibank, N.A.*, 256 F.Supp.2d 158, 163 (S.D.N.Y. 2003). Fortunately, the United States Supreme Court has made clear that a tangential relationship to a RICO enterprise is not enough to create liability; rather, **it must be shown that a bank directed or managed the illegal enterprise.** *Reves v. Ernst & Young*, 507 U.S. 170, 185 (1993). Thus a bank is not liable simply because someone who operated an illegal enterprise had accounts there. *McNew v. People's Bank of Ewing*, 999 F.2d 540 (6th Cir. 1993) (decision set forth in 1993 WL 243772 and establishing that mere participation in bank-customer relationship does not create liability under RICO).

Similar to RICO, aiding and abetting claims are improperly used against banks. In such cases, banks are sued because a third person was harmed by the tortious conduct of one of its customers. Because the third party is uncollectible, the bank becomes a target because it allegedly knew of its customer's breach of duty and assisted or encouraged the customer's conduct. See generally, Restatement (Second) of Torts § 876. **It is extremely rare that a bank actually knows of its customers' wrongdoing—and rarer still that a bank would ever encourage such conduct; accordingly aiding and abetting claims are usually without merit.**

In order to argue that a bank had actual knowledge of its customer's actions or purposefully ignored them, some plaintiffs attempt to misuse a bank's "know your customer" policies. **"Know Your Customer" policies are used by banks to help confirm the identity of new customers and to ensure they have not previously been identified as known criminals, terrorists or money launderers. The main purpose of these policies is help combat criminal money laundering and courts have consistently refused to find that such policies create a duty for banks to police their customers.** In *Holifield v. BancorpSouth, Inc.*, 2004 WL 1729492 (Miss. App. Oct. 26, 2004) victims of a Ponzi scheme involving overseas transfers of money by a bank customer argued that the bank owed the investors a duty to ferret out the fraud and prevent their losses. The *Holifield* court rejected the plaintiffs' arguments and found that **the bank's internal policies did not create a legal duty to the plaintiffs or the public at large, that banks had no duty to ensure that its customer was properly using the funds in his account.**

Banks are vital to the health of our economy and, for the protection of the public, the banking industry is one of the most highly regulated and supervised industries in the world. For tens of millions of

Americans, banks are the first choice for saving, borrowing and investing. More often than not, banks are nothing more than a conduit for transactions. Unfortunately, the things that make banks so important to our society also make them the targets of people who see them as deep pockets.

Even though such arm's length business relationships do not give rise to RICO or aiding and abetting liability, that does not keep frivolous lawsuits from being filed. These claims are brought to blackmail banks and coerce early and quick settlements based upon the notion that banks will want to avoid the defense costs required to prove they did nothing wrong. In such cases, a bank should contact an attorney who knows banking and financial institutions law. Then they can work together to combat these deep pocket claims and, hopefully, devise an early exit strategy.

Richik Sarkar is an attorney at Ulmer & Berne LLP. He focuses on complex commercial litigation with a special expertise in banking and financial institutions law, business torts, and corporate governance.

continued from page 14

the cutting edge

lawyer who provided those terms and restrictions is liable for any potential failure to find available information as well. I would check your malpractice carrier to see if providing improper search terms is covered under your policy. Second, it is questionable whether such a person can truly call themselves an expert when they are merely a keyboard monkey entering search terms provided by a non-expert. That is not a function that is beyond the knowledge of an ordinary juror. Entering search terms is likely to result in a large quantity of irrelevant data that someone is going to have to sift through to determine what is what. Finally, nothing resulting from merely entering search terms is going to capture information about computer usage.

Computer Usage

As in the age before computers, it would be a rare case indeed for someone to email, chat or otherwise keep a diary on their computer of their plan of action to carry out some criminal act or theft of trade secrets, for example. Computer analysis requires an analysis of artifacts on that machine to determine how it was used, not just what information sits on it. This can involve determining what websites were visited online, emails exchanged, logon and password information used for various sites and programs, what programs were used and for what purpose and under what username, etc. For example, I had a case with co-counsel Brandie Hawkins in which she and I hired a computer forensics firm to analyze two computers owned by a minor who it was alleged our client had intimate contact with. Our client's defense was that the minor had lied to him about her age and had done so repeatedly online and on the phone.

The analysis of her computer revealed her contact with multiple persons online claiming to be adult males and her emailing and chatting with them. During several of those emails and chats, she told each of them she was 18 years old or older. That fact, among others, were critical in obtaining a reasonable offer from the prosecutor in that case. Additional information from those computers, a select subset of which we revealed to the prosecutor as potential impeachment evidence of the alleged victim, was followed by the prosecutor dismissing the case altogether. None of that information was found by using any search terms. It was found by hard work and ingenuity by our computer forensics experts. (Email me if you want the name of the expert firm we used as I would recommend them highly).