

May 2016
Volume 42 • Issue 3

Banknotes

Ten Strategies
to Avoid Selling
Your Bank

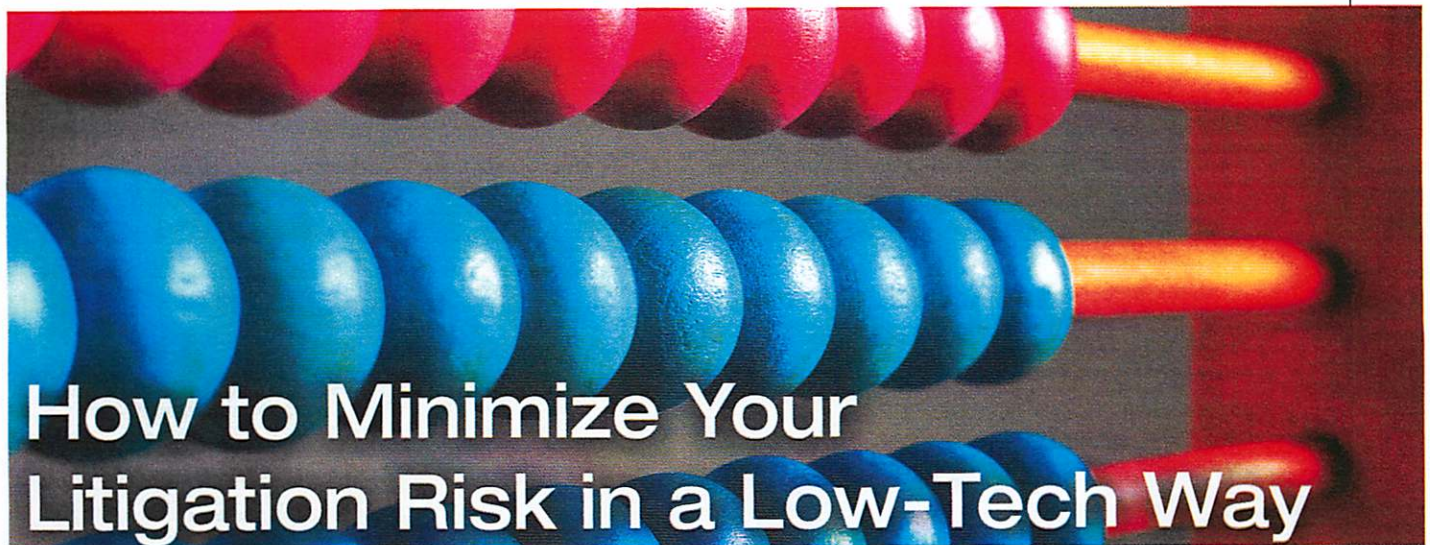
page 09

What Makes
Great Boards Great

page 10

CBAI Foundation
for Community
Banking Turns 20

page 26



How to Minimize Your Litigation Risk in a Low-Tech Way

Cathy Ghiglieri, President, Ghiglieri & Company, Austin, TX

Ten years ago, I wrote an article for *Banknotes* on how banks could minimize their litigation risks. Unfortunately, many of the same schemes are present today as they were 10 years ago, such as check fraud, check kiting, elder abuse, bookkeeper fraud, and construction loan fraud. Today, cybersecurity and other high-tech risks are consuming bankers' attention in order to reduce their operational and reputational risks. While these issues are important, here are a few of the low-tech ways in which banks can minimize their litigation risk.

1. Policies and procedures:

All banks should have written policies and procedures for every area of the bank. In order to minimize litigation risk, there should be a process to ensure that bank employees are complying with these policies and procedures. Policies and procedures covering the area being litigated will often be requested, and a comparison of the bank's actions to the policies and procedures will often be made as part of the litigation. Being able to show that the bank has adequate policies and procedures and that bank employees complied with them will help to minimize litigation risk.

2. Bank Secrecy Act and automated account monitoring systems:

Bank Secrecy Act/Anti-Money Laundering (BSA/AML) compliance is a major focus of bank examinations today as it has been over the last 10 years, and compliance with the Bank Secrecy Act can have the added benefit of minimizing litigation risk. Automated account monitoring systems are extensively discussed by the Federal Financial Institutions Examination Council ("FFIEC") in its BSA/AML Examination Manual. Automated account monitoring

systems generate alerts when account transactions exceed certain parameters. These alerts help the bank identify a fraudster's activities and suspicious transactions.

Banks that ensure that their BSA investigators are highly trained to investigate these alerts and identify suspicious activity minimize their litigation risk. These systems alert for a reason, and making sure that alerts are not ignored or misinterpreted can help identify suspicious activity and stop fraudulent activity in its tracks. Money laundering, including Ponzi schemes, can be detected when alerts are properly and timely investigated.

3. Teller transactions:

Tellers are the first line of defense for the bank in preventing fraud and in minimizing its litigation risk. While tellers are not the highest paid personnel in the bank, they can often prevent thousands, even millions, of dollars in litigation expenses and/or settlement amounts in the manner in which they cash checks, take deposits, issue cashiers checks, and change addresses on accounts. Here are some examples:

- A company bookkeeper wants to cash a check drawn on a corporation, a common type of bookkeeper fraud. Many banks have a policy against cashing checks drawn on corporate accounts. This procedure can prevent bookkeeper or other types of fraud.
- A company bookkeeper wants to deposit a check made payable to his employer, ABC Corporation, into his personal account, another common type of bookkeeper fraud. Many banks refuse to deposit checks made payable to corporations to other than the corporate account matching the name of the payee. This requirement prevents bookkeeper or other types of fraud.

- A customer wants to obtain a cashiers check, but doesn't not have sufficient collected funds in the account to pay for it: Banks should have policies and procedures to require that the payment for cashiers checks are drawn on collected funds, instead of uncollected funds. Otherwise, the bank is paying for the cashiers check with its own funds and it is potentially making an unsecured loan to the customer should the funds never become collected without going through the bank's stringent underwriting process. In many cases, these cases require litigation in order to collect payment.
- A fraudster pressures an elderly person to cash in a Certificate of Deposit prior to maturity in order to access the funds, a common type of elder abuse: The bank should have teller policies and procedures that address when an elderly person requests to cash in a Certificate of Deposit prior to maturity, in order to identify whether elder abuse, defined as the illegal or improper use of an older adult's funds, property or assets, is taking place.

Having written policies and procedures for all of these types of transactions, and making sure tellers are following them, can minimize litigation risk, and prevent bookkeeper fraud, elder abuse or other type of fraud.

4. New Accounts Department:

The manner in which a bank opens a new account can stop a fraudster from ever using the bank to perpetrate a fraud by utilizing robust customer due diligence and customer identification procedures required by the Bank Secrecy Act. Here are some examples of how the new accounts department can stop a fraud before it begins:

- A fraudster attempts to open a corporate account with little or no documentation: The bank should have procedures to prevent an account from being opened without proper documentation. Customer due diligence procedures should include a check with the Secretary of State's website to determine if the corporation even exists, who the officers are, and customer identification procedures should ensure the person requesting the new account has the proper authority to open the account.
- A company bookkeeper attempts to open an account using a name that closely resembles the name of the company for which the bookkeeper works in order to redirect company checks into this account, a common bookkeeper fraud: Having procedures that require a check with the Secretary of State's website to determine if the company exists, if there are similarly named companies, and who the officers are can prevent bookkeeper fraud from even starting.

- A fraudster wants to add their name to an existing account or to change an address on an existing account, common elder abuse tactics: Performing customer due diligence, such as contacting the account holder to confirm these changes or requiring that the account holder be present before changes can be made, can prevent such things as elder abuse or other types of fraud.

Adhering to the requirements of the Bank Secrecy Act for opening new accounts or making changes to existing accounts can help prevent bookkeeper fraud, elder abuse, money laundering, and minimize litigation risk. Utilizing post-account opening or post-account change review procedures can also help catch problems before they begin.

5. Manual account monitoring reports:

The FFIEC discusses manual account monitoring systems in its BSA/AML Examination Manual to include uncollected funds reports, overdraft reports, large balance reports, check kiting reports, large item reports, and wire transfer reports. These reports are low-tech ways of identifying suspicious activity, including check kites, money laundering, Ponzi schemes or other types of frauds. Accounts that routinely show up on these reports should be investigated to ensure that suspicious activity is not taking place and to help minimize litigation risk.

6. Construction loans:

The regulators have issued recent guidance on concentrations in commercial real estate loans and banks are again making more construction loans. This is an area that can be ripe with fraud. Controls for construction loans should be in place including how construction loans are monitored, how draws are controlled, when inspections are required and by whom they are made, how construction draws can be obtained by the borrower, and what documentation is required prior to advancing construction draws. Having these policies and procedures in place and ensuring loan officers adhere to them will help minimize litigation risk.

While high-tech risks deserve the banks' attention, these are some of the low-tech methods that banks can use to minimize litigation risk. ■

Ghiglieri is the former Texas Banking Commissioner and is president of Ghiglieri & Company, a bank consulting firm based in Austin, TX. She is the co-author of "The Ultimate Guide for Bank Directors, Revised Edition (2015)". Contact her at cathy@ghiglieri.com or visit her website at www.ghiglieri.com.