JUNE 2016

IB

INDEPENDENTBANKER.ORG

+ THE BIG ISSUE

» Big-Growth Banks Tell Their Stories
+ Top-50 Fastest-Growing Community Banks

» Big Ideas for Today and Tomorrow

ICBA

CHIEF Architect

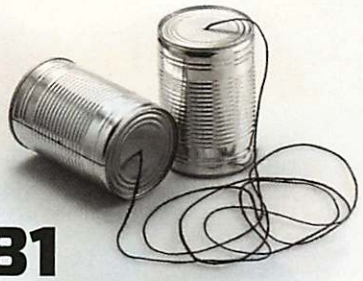
Linda Echard built community banking's payments powerhouse

contents » departments

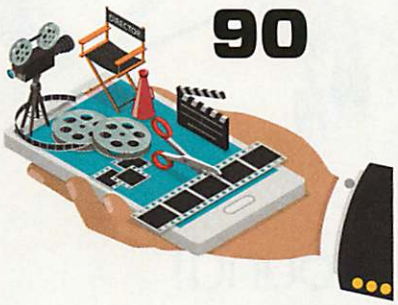
Grassroots

Lender Life

Risks & Rules



Nuts & Bolts



Back Page

IB
WWW.INDEPENDENTBANKER.ORG

ICBA
Independent Community Bankers of America®

ICBA HEADQUARTERS/EDITORIAL OFFICE

1615 L St. NW, Suite 900
Washington, DC 20036-5623
Email: magazine@icba.org
(202) 659-8111
(800) 422-8439

www.icba.org
www.facebook.com/icbaorg
www.twitter.com/icba

VOL. 66 No. 06

Periodicals postage paid at Sauk Centre, MN, and additional mailing offices. *ICBA Independent Banker* (ISSN-0019-3674) is published monthly by Independent Community Bankers of America, 518 Lincoln Road, Sauk Centre, MN 56378-1653. Member subscriptions, $40 per year. Additional member subscriptions, $20. All other subscriptions, $75. POSTMASTER: Address changes to *ICBA Independent Banker*, P.O. Box 267, Sauk Centre, MN 56378.

» PAYMENTS EXCHANGE

Procedural Protection

Routine, low-tech practices that minimize transaction fraud

By Cathy Ghiglieri

Ten years ago, I wrote an article on how community banks could minimize fraud losses. Unfortunately, many of the same criminal schemes are present today as they were then, such as check fraud, check kiting, elder abuse and bookkeeper fraud. Today, threats to cybersecurity and other high-tech risks are consuming bankers' attention to reduce their operational and reputational risks.

Although high-tech solutions are important, here are a few of the low-tech ways in which community banks can minimize their fraud losses.

1 Policies and procedures. All banks should have written policies and procedures for every operational area and a process to ensure that employees are complying with them. This allows banks to identify weaknesses and

p. 84 » Tech Talk

p. 86 » Cyberworld

p. 88 » Portfolio Management

p. 90 » Marketing Today

inconsistencies in the application of their policies and procedures and to identify places where detection of fraud may need to be strengthened.

2 Bank Secrecy Act and automated account-monitoring systems.

Bank Secrecy Act/anti-money-laundering compliance is a major focus of bank examinations today, as it has been over the last 10 years. The Federal Financial Institutions Examination Council extensively discusses automated account-monitoring systems in its BSA/AML Examination Manual. Automated account monitoring systems should generate alerts when account transactions exceed certain parameters. These alerts help banks identify fraudulent activities and suspicious transactions.

Banks should ensure that their BSA investigators are highly trained to investigate these alerts and identify suspicious activity to minimize fraud losses. Making sure that account-monitoring system 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 a bank in preventing fraud. Although tellers are not the highest paid personnel, they are best positioned to identify fraudulent transactions first while cashing checks, taking deposits, issuing cashier's checks and changing addresses on accounts.

These typical bank policies for frontline tellers will help prevent common fraudulent transactions:

» 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 Corp., into his personal account, another common type of bookkeeper fraud. Many banks refuse to deposit checks made payable to corporations into accounts that do not correspond to a corporate account matching the name of the payee. This requirement helps prevent bookkeeper or other types of fraud.

» A customer wants to obtain a cashier's check, but does not have sufficient collected funds in the account to pay for it. Banks should have policies and procedures to require that the payment for cashier's checks are drawn on only collected funds, instead of uncollected funds. Otherwise, a bank is paying for the cashier's 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. Often these cases require litigation to collect payment.

» A fraudster pressures an elderly person to cash in a certificate of deposit prior to maturity to access the funds, a common type of elder abuse. Banks 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.

4 New accounts department.

The manner in which a bank opens a new account can stop new-account fraud by using robust customer due diligence and customer identification procedures required by the Bank Secrecy Act. The following 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. Banks 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 and who the officers are. Customer identification procedures also 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 his or her 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.

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.

Cathy Ghiglieri (*cathy@ghiglieri.com*), a former Texas banking commissioner, is president of Ghiglieri & Co., a community bank consulting firm in Austin, Texas. She is the co-author of *The Ultimate Guide for Bank Directors, Revised Edition* (2015).