TECHNOLOGY AND FINANCIAL CRIMES

by Steve Brown

We are living in the Technology Age where most things are within our reach simply with the click of a mouse or a voice command. Millions of transactions are done on a daily basis via the internet. Globalization and interconnectivity has enabled us to reach across seas and into exotic lands, while sitting at home or in a cafe' to transact business. Many financial institutions are also using the internet to connect with customers, for advertising and promoting new products. Community banks are taking advantage of this online explosion as a marketing tool not only to retain existing customers but to capture new ones, increase loans or deposits and promote new products with appealing features. For many people it is easier and faster to open an account on the internet, rather than standing and waiting in a line at the bank. It is more convenient, fits a busy schedule and often requires fewer forms or disclosures to read and complete. Just as the internet provides opportunity, so too does it pose a threat to banks. Faceless crooks abound, using technology to set-up accounts for money laundering or conduct other financial crimes. How well do you know the person or entity you are banking, when you have never met them face to face? What steps should you take to ensure that your potential client is safe and how do you "know" them? All bankers understand knowing your customer (KYC) is vital to ensure that relationships are strong and safe. A good Customer Identification Program (CIP) was introduced by regulators to help safeguard the system, prevent or decrease fraud, money laundering and combat the funding of terrorists. It is standard practice now for each person who requests you to open an account for them be identified with standards that require four key pieces of information such as name, date of birth, address (physical address-no postal boxes) and an identifying number such as social security. For business entities, valid licenses, recorded documents, articles of incorporation and trust documents are required and must be verified at the time of opening the account. Prudent bankers follow policies and procedures when identifying customers and make sure all boxes are properly checked as part of the process. Verifying each individual or entity and utilizing available government resources to assist in the verification process make sense and are used often by community bankers. For example, the Office of Foreign Asset Control (OFAC) site may be used when opening an account to ensure the individual or entity listed isn't an issue and name searches may be matched against other listings such as the Political Exposed Persons list (PEP). By reviewing and comparing OFAC results carefully, banks are protected and integrity in the process is maintained. Educating and training employees to follow OFAC procedures, understand which countries or organizations are sanctioned and avoiding issues just makes sense. No one wants to pay fines or have bad publicity, so reminding staff, updating policies and procedures and testing compliance are good practices. Doing so will ensure your bank is not only efficient, but ultimately prevents money laundering and other financial crimes.

Related Links:
PCBB 2013 Executive Management Conference

BANK NEWS

State Fraud

The New York Times reports the state of Illinois settled with the SEC after misleading bond investors by failing to disclose it was underfunding its pension system.

Fewer Branches

SNL reports the total number of in-store branches has declined 4.6% since June 30, 2011.

Competition

Wells Fargo announced it plans to lend $55B to women-owned businesses by the end of 2020.

Job Cuts

Regions Financial announced it reduced its staff headcount by 280 positions in 2012 or about 1.1%.

Mobile Risk

The Federal Trade Commission (FTC) released a study that projects in the next 2Ys mobile payments will "achieve widespread mainstream consumer adoption." The FTC used the report to highlight concerns about security, privacy and how disputes are resolved by mobile carriers. In particular, the FTC warned people to tie mobile payment options to credit cards, since specific liability regulations apply to fraudulent credit card charges ($50 if reported in 2 days and $500 if reported after 2 days), but do not apply to debit or reloadable/prepaid cards (where liability is potentially unlimited).

Customer Survey

A new survey by TD Bank finds 60% of consumers who are happy with their bank say they have low or no financial stress and this same group spends 72 minutes less each week worrying about their financial situation (vs. the unhappy group). Meanwhile, 75% of those aged 18-34 said friendly service was key to an ideal banking relationship vs. 82% for those aged 35-54 and 89% for those 55+.

Trading Multiples

SNL reports the price to tangible book multiple for small cap public banks they track (with assets $250mm to $1B) has fallen from 2.33x in 2007. It dipped to 1.97x in 2008 and has since bounced around at 1.40x in 2009, 1.58x in 2010, 1.33x in 2011 and 1.46x at the end of 2012.

Capital

A new proposal from the International Accounting Standards Board (IASB) is expected to go into effect in 3Ys and would require banks to set aside provisions for current loans based on likely loss over the next 12 months and to take provisions totaling the full expected loss on loans more than 30 days delinquent. The change is expected to increase reserves.