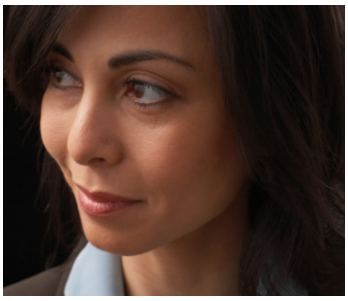

MINI-CASES

OPERATIONAL RISK EVENTS

JOIN.
ENGAGE.
LEAD.

CASE #1

In 2004, a $25 million fine levied against Riggs National Bank for violating anti-money laundering and bank secrecy laws sent shockwaves through the industry and led directly to the sale of the bank. Riggs' relatively unusual business model (including international banking services for the likes of Chilean dictator Augusto Pinochet) led many bankers to assume that the incident was not really relevant to their institutions.

But later that same year AmSouth Bank, an institution with a more traditional banking business model, was fined $50 million for violating anti-money laundering and bank secrecy laws. The findings stemmed from an incident in which two men who had been running a Ponzi scheme were caught and sentenced to long prison terms. Victims of the scheme lost a total of $10 million, virtually all of which was recovered through civil litigation.

AmSouth's involvement stemmed from the fact that money involved in the scheme was funneled through the bank. Regulators considered AmSouth culpable because they felt it should have identified and reported the scheme. AmSouth exacerbated the problem by failing to respond to eight subpoenas issued by the grand jury investigating the scheme, and providing government attorneys with responses that were considered "misleading and inadequate".

In addition to the $50 million fine, AmSouth agreed to revamp its procedures and to forgo a planned expansion. The bank remained subject to criminal prosecution if the U.S. Attorney's office was not satisfied with its progress.

Ultimately, AmSouth merged with Regions Financial in 2006. The price paid by Regions was below the price at which AmSouth shares were trading at the time of the announcement. While the 2004 incident did not lead directly to the merger, there is little doubt that the terms of the settlement with the U.S. attorney stunted AmSouth's growth plans and ultimately impacted the terms of the merger.

CASE #2

In a case which stunned co-workers and customers, two employees of Bank of America in Austin, TX pleaded guilty to stealing $2.6 million from the bank and five of its predecessors over a 23-year period.

The women, who began as tellers in 1975, rose through the ranks of Austin National Bank, InterFirst Bank, First Republic Bank, NCNB Bank, NationsBank and finally Bank of America as the banks for which they worked were acquired time and again by larger institutions.

The women stole the money in small increments (typically $2,500) over a long period of time by taking cash from the vaults they controlled and manipulating bank records. One of the women was a customer service manager, while the other was teller manager of a drive-through branch several blocks away.

While complete details of the scheme will never be known, prosecutors said that the scheme involved false accounting and manipulation of records of cash transfers between the vaults of the two branches, and that their approach changed over time as the banks changed hands and the women gained additional responsibilities.

The women had reputations as tough, by-the-book supervisors. Over the years, they refused promotions and transfers, and planned their vacations to ensure that the fraud was not uncovered. Their strategies worked until Bank of America introduced a new computer system which identified differences between vault cash and ledger balances.

A federal judge sentenced the women to 5 years and 10 months in prison in addition to 5 years probation. The women were also ordered to repay the stolen money, although given their relatively modest means and the fact that the funds were apparently spent on routine household expenses prosecutors consider it unlikely that the money will ever be repaid.

CASE #3

Two Baltimore-area banks suffered large losses as the result of a check kiting scheme orchestrated by a money services business.

Carrollton Bancorp, with $350 million in assets, reported an after-tax loss in excess of $1 million, while $800 million asset BCSB Bankcorp took an after-tax charge of nearly $7 million. A third bank, $161 million asset Farmers and Mechanics Bank, also maintained a relationship with the money services business, although Farmers and Mechanics claimed not to have lost money in the fraud.

The fraud was perpetrated by the owners of a Baltimore-based check cashing firm. The owners, who held leadership positions in trade groups and associations, originally began kiting checks to cover a shortfall caused by the settlement of a lawsuit. Over the course of a three year period the amounts were increased in order to fund the opening of new check cashing locations and pay owners salaries.

The process was fairly straight-forward; each day, the owners would check their true balance position and deposit checks sufficient to cover any shortfalls. By depositing checks drawn on one bank in the account of another and vice-versa, they were able to write checks in excess of the funds actually on deposit. The owners wrote hundreds of checks for millions of dollars in order to keep the fraud going.

The collapse of the kiting scheme resulted in very large losses for the banks, and BCSB was forced to raise additional capital in order to remain viable. One of the owners committed suicide as the scheme unraveled, and his brother was eventually sentenced to 3 years in prison followed by 4 years of supervised release and was ordered to make restitution to the banks.

CASE # 4

In a case that stemmed from multiple breakdowns, Canadian Imperial Bank of Commerce (CIBC) was sued by a West Virginia scrapyard operator for $3 million. In addition to the litigation, the story received considerable press in both the United States and Canada and negatively impacted the bank's reputation.

The incident resulted from a mis-published fax number distributed to CIBC offices across Canada. Based on the error, funds transfer requests containing social security numbers, bank account numbers, and other non-public information was faxed to the West Virginia scrapyard rather than their intended destination within the bank.

The situation was compounded by the bank's inadequate response to complaints from the scrapyard operator about the misdirected faxes. Frustrated by the lack of action on the part of the bank to address the situation, the owner of the scrapyard took his concerns to the press, and to the courts. Once the situation became public, the bank's position was further undermined by the fact that it had failed to notify the individuals whose information had been compromised about the situation.

The scrapyard received faxes from approximately 350 phone numbers inside Canada over a 3 year period. The owner claimed that, in addition to the breach of non-public information, the fax traffic disrupted the dealings of his auto accessories business.

The Canadian Office of the Privacy Commissioner became involved following the revelation of this incident and a similar one which came to light soon after. The Commissioner found that the breaches were the result of inadequate operational and management policies and stated that "the bank's privacy practices were seriously tested by these incidents and they failed". The bank accepted the findings and agreed to a series of actions including the creation of a National Privacy Office and the establishment of a national database and process to track and address privacy issues.

CASE #5

In a case that highlighted the dangers of aggressive sales promotion without adequate compliance mechanisms, Citizens Bank agreed to refund fees and pay a fine to the state of Massachusetts.

The settlement resulted from findings that employees of Citizens and its broker-dealer subsidiary targeted senior citizens over the age of 75 for aggressive variable annuity sales pitches. Variable annuities are considered unsuitable for older individuals based on their volatile market values and high fees for early withdrawal.

Investigators found that Citizens employees cold-called senior citizens with CD balances in an effort to convince them to move their money to the more volatile, higher-fee annuities, which also lacked FDIC insurance. Successful salespeople from the bank as well as the broker-dealer were rewarded with trips to the Caribbean and other destinations as well as expensive tickets to concerts and sporting events. Citizens was also unable to produce employee emails subpoenaed by the state.

In addition to agreeing to offer full refunds to all of its customers who were 75 or older at the time they purchased the annuity, Citizens terminated a number of employees and agreed to pay a $3 million fine. In addition, the bank admitted to the Secretary of State's finding that it engaged in "unethical or dishonest conduct". The SEC also initiated an investigation of Citizens variable annuity practices.

CASE #6

Birmingham, AL-based Compass Bank agreed to pay more than $1 million in back overtime wages to nearly 3,000 employees following an investigation by the U.S. Labor Department that determined the company had violated the Fair Labor Standards Act (FLSA).

The FLSA requires that employers pay covered workers at least minimum wage, as well as 150% of the regular pay rate for all hours worked over 40 in a single work week. The law also requires employers to maintain accurate records of employees' wages, hours and other conditions of employment.

Federal investigators found that over the course of two years tellers, customer service representatives, and financial services representatives at Compass branches in six states routinely worked through lunch and after scheduled hours. The employees spent the extra work time balancing accounts, preparing required paperwork, attending meetings, and calling customers. However, the bank failed to record the extra time as work time and failed to compensate workers.

The investigation began at a few branches in Alabama. After violations were discovered in those branches the investigation was expanded to cover Compass locations elsewhere. The root causes appear to be that the bank's time-keeping system defaulted to eight hours unless corrected by the employee and that many supervisors did not understand what counts as "paid time" and encouraged employees to work off the clock.

The Labor Department cited the bank's cooperation with the investigation, which in all likelihood mitigated the risk of more significant penalties.

CASE #7

In a case of people and external risk, fifteen million dollars was illegally withdrawn from accounts with the Municipal Credit Union of New York City in the days after the tragic events of September 11, 2001. The Credit Union – which counts among its client base police officers, teachers, and firemen -- suffered a computer failure after the collapse of the World Trade Center towers, and allowed its clients limited access to its automated teller machines as a service during a difficult time. The Credit Union was across the street from the World Trade Center and lost its connection to the New York Cash Exchange ATM network. The network had no way of insuring that when credit union clients withdrew money from ATM machines that there was sufficient money in their accounts to cover the transactions.

The Credit Union claimed that it operated under these tenuous conditions because it did not want to refuse 300,000 clients access to their money during a horrific time in the city. However, it appears that a number of clients abused this situation. One city employee who never had an end-of-the-month balance that exceeded $130, made 53 ATM withdrawals ranging from $20 to $300 each, and charged 101 Visa purchases using his credit union card between September 19th and October 22nd. His account balance was overdrawn by over $10,000 by the end of October 2001.

Arrest warrants were issued for more than one hundred people who withdrew $7,500 or more beyond what was in their accounts, and an estimated 4,000 people were suspected of smaller frauds. All of those investigated overdrew their accounts by at least $1,000 and refused offers from the city to pay back their overdrafts through loans at reduced interest rates.

The Credit Union was eventually able to trace the overdrawn cash withdrawals by undisclosed methods. The amount of money illegally withdrawn from ATM machines during a time when “people tried to profit from the confusion” is estimated to be in the range of $15 million. According to the Credit Union it went out of its way to create an atmosphere of orderliness during a time of great trauma and was victimized by people who took advantage of the situation.

CASE #8

In two cases which resulted in credit charge-offs but stemmed directly from operational risk events, National Penn Bancshares lost $11.2 million due to loan frauds by internal employees.

In the first episode, the bank lost $6.7 million of gross revenue due to a "pyramid-style scheme" involving identity theft and loan fraud. The $4.5 billion asset, 130 year-old institution also spent in excess of $600,000 on its internal investigation and was forced to delay release of its quarterly and annual financial statements.

The fraud was perpetrated by a mid-level banker and involved stealing the identities of customers and relatives, forging loan applications, tax returns, financial statements, checks, and other documents, and pocketing the proceeds of fictitious loans approved on the basis of the falsified paperwork. He also used his authority to waive overdraft fees when loan payment checks bounced.

The lender, who allegedly lived a lavish lifestyle with the help of the loan proceeds, also initiated fraudulent loans on behalf of a local orthodontics practice. The dentists had allegedly threatened to reveal the fraud unless the banker also obtained loans for them, which he did on multiple occasions.

The lender was also allegedly aided by two co-workers, who called to warn him that bank auditors were on the way and helped him to destroy incriminating documents. In the wake of the event, the bank tightened its examination procedures as well as its practices for verifying customer identities and signatures.

The second event, uncovered nearly four years later, involved a retail loan operations manager with 27 years at the bank. Once again, the scheme involved the fraudulent opening of lines of credit and the transfer and theft of funds from the fraudulent loans. She also used her system access to delete accrued interest associated with the loans. Overall, nearly $4.5 million was stolen from the bank.

The manager used the funds to purchase four homes for herself and family members, as well as cars, furniture, jewelry, and other items. Some of the money was used to fund bank and investment accounts.

In both cases, the bank sued the employees and won restitution, although it is unclear whether all of the funds will eventually be repaid. Each of the bankers was convicted and sent to prison.