

LESSONS TO BE LEARNT FROM THE WORLD'S BIGGEST BANKING FRAUD – SOCIETE GENERALE

Anand Prakash Jangid
ACA, CISA, DISA, CISM, ACP.

Abstract: This paper analyzes the events that led to the €4.9bn (\$7.2bn) fraud at Societe Generale that made headline news items around the world during the recent past. It looks at the different control failures which led to the Societe Generale fraud and talks about the importance of enterprise wide risk management and how it needs to be implemented.

1. Introduction

How could this possibly have happened? That was the question being asked in financial circles worldwide Jan. 24, after France's Société Générale (SocGen), one of Europe's biggest banks and a global superstar in the booming derivatives-trading business, disclosed a staggering \$7.1 billion loss from rogue trading by a single employee.

One of France's oldest banks, Société Générale was chartered in 1864 by Napoleon III and is now the country's second largest publicly traded financial institution, well-known for its extensive and heretofore sophisticated derivatives trading operation.

The simple answer is this: One of the biggest frauds in financial-services history apparently was carried out by a 31-year-old trader in Société Générale's Paris headquarters, whom multiple news sources have identified as Jerome Kerviel. The trader "had taken massive fraudulent directional positions"—bets on future movements of European stock indexes—without his supervisors' knowledge, the bank said. Because he had previously worked in the trading unit's back office, he had "in-depth knowledge of the control procedures" and evaded them by creating fictitious transactions to conceal his activity.

2. Previously, Double-Digit Growth

While those facts seem fairly straightforward, a host of troubling questions still need to be answered: How could SocGen, which ironically was just named Equity Derivatives House of the Year by the financial risk-management magazine *Risk*, have failed to detect unauthorized trading that it acknowledges took place over a period of several months? Do banks need to tighten the controls put in place after rogue trader Nick Leeson brought down Barings Bank in 1995? Or is the red-hot business of equities-derivatives trading just too tricky to control?

SocGen's equities-derivatives business, the biggest at any institution in the world, has posted double-digit growth the past eight years and until now has been hugely profitable. Fitch estimates the business generated about \$1.7 billion in profits during 2006, or about 20% of the bank's net earnings. Backed by elaborate algorithmic models, trading instruments with exotic names such as Himalaya and Altiplano have generated an average 40% return on equity for the bank, more than twice the rate for its retail banking business.

Yet SocGen's derivatives operation is relatively small, with fewer than 2,500 employees including about 300 traders and roughly 750 middle- and back-office employees, according to a 2006 investors' presentation by the bank. The rogue trader apparently spent several years in a back-office job before realizing a long-held dream of moving to trading.

3. Inadequate IT security

Between Jan. 18 and Jan. 20, the bank discovered that trader Jérôme Kerviel had established trading "positions" -- bets that the price of securities and warrants would move in a particular direction -- worth more than the bank itself. He bet wrongly, and unwinding those positions over the following three days cost the bank €4.9 billion as it sold the stocks into a falling market.

As an arbitrage trader, Kerviel should have been making transactions in pairs, buying and selling similar assets to exploit the minute and fleeting differences in prices that exist in markets. Arbitrage trading is considered less glamorous than the one-way bets he secretly made from time to time by faking one half of a pair of transactions. Kerviel had previously worked in the bank's IT department, and so had in-depth knowledge of its systems and procedures. Staff mostly followed those procedures, the investigating committee found, but the procedures were

not in themselves sufficient to identify the fraud before Jan. 18, partly because of the effort Kerviel made to avoid detection, and partly because staff did not systematically conduct in-depth investigations when warnings flags were raised.

Among the tricks Kerviel used to hide his activities, the bank's General Inspection department highlighted the use of fake e-mail messages to justify missing trades, and the borrowing of colleagues' log-in credentials to conduct trades in their name. Investigators identified at least seven occasions on which Kerviel faked messages between April 2007 and Jan. 18, four of them referencing trades that never existed. The deception was eventually uncovered when they could find no trace of Kerviel receiving the purported messages in the bank's e-mail archival system, Zantaz. Between July 2006 and September 2007, internal control systems raised 24 alerts when the value of Kerviel's trades exceeded authorized limits, the General Inspection department reported. At the time, the bank's risk monitoring unit put the anomalies down to recurrent problems with the way the trading software recorded operations, and asked Kerviel's superiors to make sure he didn't exceed limits again.

4. Conclusion

The special committee made a number of recommendations, including the use of stronger, biometric authentication systems to prevent traders from accessing one another's accounts, and the improvement of alert procedures so that warnings reach the appropriate managers. In addition, it suggests the tightening of trading controls, which do not cover canceled or modified transactions, two of the tricks Kerviel used to conceal his bets. To prevent a recurrence, the bank should immediately introduce stronger security systems, including biometric authentication of trading staff, a special committee has recommended in its preliminary report to the bank's board of directors. With more frauds happening today with the help of Information system, it calls for better IT controls over different business function.