

**Have we really learned
anything from the GFC ?**

Dr. Tony Coleman

Lonergan Edwards & Associates

Macquarie University Financial Risk Seminar

22 March 2013

Introduction

- Risk Management 101:

You do not need a parachute to skydive.

(you only need a parachute if you want to do it twice)

Introduction (Cont.)

- It is now nearly 5 years since Lehman Bros collapsed at the start of the GFC
- Many millions of words have been written about the consequences of the GFC
- Many initiatives have been discussed and some even taken world-wide to prevent a repetition
- But we are still living with many of the consequences
- Are we going to avoid making these mistakes again ?

Regulatory Response

- Banking regulators have responded with:
 - higher capital requirements
 - new liquidity rules, and
 - mandated maximum leverage
- But will these measures enhance a bank's abilities to identify and manage low frequency/high severity risks ?
- Probably not - they are more like an "airbag"
 - designed to cushion the impact, rather than
 - designed to avoid an accident altogether

Some causes of risk

- Lack of firms (and their regulators) thinking systemically –
“ What if everyone else is doing the same as I am - will we be trampled by the herd ? ”
- “As long as the music is playing, you’ve got to get up and dance. We’re still dancing...”
- “You can only be as good as your dumbest competitor.”
- “Bad news travelling slowly”
- “Shooting messengers (mainly inside organisations)”

Behavioural risk - a CRO's dilemma

- Suppose a CRO is convinced there is a market bubble about to burst or an unacceptable level of risk in an activity
- What actions can the CRO take to protect the firm ?
 - **Get firm to exit or reduce activity in the exposed business** - but why will management want to give up the firm's profitable market share in a business (and probably lose talented and expensively-recruited top-performing staff) ?
 - **Implement hedging strategy using derivatives** - but if the CRO recognises the problem "too early" (say in 2006 for CDOs) this will result in such large losses that the CRO would probably be fired
- What would you do if you were the CRO with this dilemma ?

Some Recent Risk Event Examples

Let us now look at some recent risk events to see :

- what we have learned,
- how much we still have to learn, and
- what still needs to be done !

1. Barclays (& others) – LIBOR Jun 12

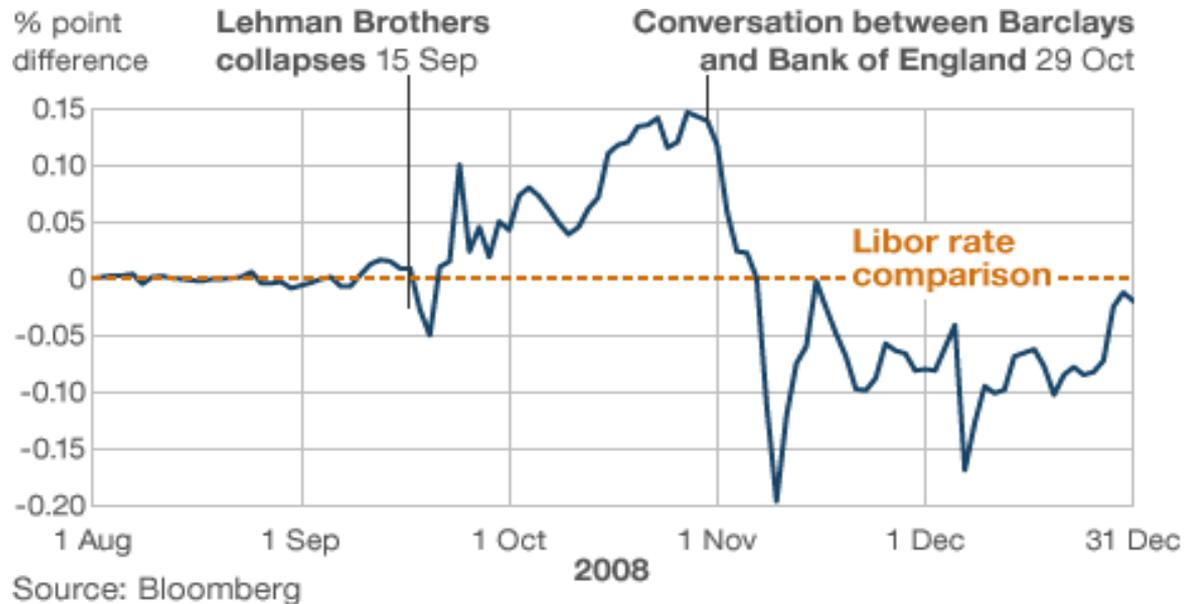
- LIBOR is used to set interest rates for some \$300 trillion (\$300,000,000,000,000) of balances (equivalent to about 4.5 x Global GDP)
- Banks submit estimates of what they would pay other banks to borrow (10 currencies /15 maturities)
- Top and bottom quartiles are discarded and average of the rest was calculated to fix LIBOR
- Since estimates were submitted rather than transactions, it was easy to submit false figures

Barclays (& others) - LIBOR

- Because LIBOR is used in US derivatives markets, manipulating LIBOR is a violation of American law
- Evidence exists that shows both New York Fed and Bank of England knew banks were “not posting honest LIBOR” as early as 2007
- Barclays was fined US\$452 million :
 - \$200 million by Commodity Futures Trading Commission
 - \$160 million by US Department of Justice
 - \$ 92 million by the UK Financial Services Authority

Barclays (& others) - LIBOR

Barclays LIBOR 3 Month Sterling submissions vs daily LIBOR fix



Barclays (& others) - LIBOR

- Barclays manipulated rates for two reasons:
 - from as early as 2005, to benefit the positions taken by the banks traders
 - from 2007 to 2012, to make the bank look healthier during the global financial crisis
- Both Chairman & CEO of Barclays resigned
- UBS agreed to pay fines to US, UK and Swiss regulators totalling \$1.2 billion in December 2012
- RBS also fined heavily, from employee bonus pool

Barclays (& others) – LIBOR

- Estimates of cost of manipulated LIBOR to US State & Local Govt. borrowers are \$6 – \$10 Billion
- British Bankers Association agreed to transfer oversight of LIBOR to UK regulators
- In future, banks submitting rates will be required to:
 - base the rates on actual transactions and keep auditable records supporting their submissions
 - make submissions publicly available after 3 months

2. Knight Capital – August 2012

- \$458 million loss from a computer malfunction
- Knight represented about 10% of US share trading
- Malfunction caused share trading volume to increase and prices to become volatile
- Knight Capital share price plunged 75% in 2 days
- Former shareholders lost 70% of their equity in subsequent \$400 million recapitalisation

Knight Capital

- Loss reportedly stemmed from an old set of computer programs that were inadvertently reactivated when a new program was installed
- Once triggered on August 1, the dormant system started multiplying stock trades by one thousand
- Many trades executed in error had to be subsequently cancelled
- Knight formed a Risk Committee after the event and created trading controls to enable a faster response to any future trading errors

3. HSBC & Money Laundering - 2012

- Agreed to pay a fine of \$1.9 billion to settle a US Money Laundering legal action in December 2012
- HSBC was accused of transferring some \$16 billion of funds over 6 years:
 - through the USA on behalf of Mexican drug cartels
 - for “rogue” nations such as Iran that are subject to international sanctions (supported by 180 countries)
- HSBC was accused not merely of lack of oversight or incompetence, but of wilful negligence - taking steps to aide and abet the financing of terrorist organisations and hide it

HSBC & Money Laundering

- Regulators were also at fault. Prior to 2010, the Office of the Controller of the Currency (OCC) had cited HSBC for many anti-money laundering deficiencies
- OCC knew HSBC had a large backlog of unreviewed accounts and that HSBC had failed to file many “suspicious activity” reports
- But OCC had not taken any enforcement action against HSBC in the previous six years

HSBC & Money Laundering

- HSBC was not alone. Since 2009, banks fined for facilitating transactions with Iran, Libya, Sudan and Myanmar include:
 - Standard Chartered
 - ING
 - Credit Suisse
 - Royal Bank of Scotland
 - Lloyds Bank, and
 - Barclays
- HSBC's fine was about 9% of one year's profits
- But no-one has gone to jail – are banks “too big to jail” as well as “too big too fail” ?

4. J P Morgan & the “London Whale”

- Some \$6.2 billion lost in 2012 from trading in Credit Default Swaps (CDS) (conceptually similar to AIG in 2008)
- JPM Shares lost 20% of their value in the month following announcement of the loss on 11 May 12 (a loss of some \$30 billion in market capitalisation)
- J P Morgan publicly issued a 129 page report summarising :
 - what happened
 - how it happened
 - remedial measures taken by J P Morgan – lessons learned

J P Morgan – What happened

- The Chief Investment Office (CIO) of JPM was responsible for managing a Synthetic Credit Portfolio (SCP) which was intended to offset some of the credit risk assumed by JPM in its capacity as a lender
- The SCP was composed of both long and short positions in credit default swap indices and related instruments
- In simple terms, buying/(selling) positions in CDS indices is analogous to buying/(selling) insurance on credit risk presented by groups of companies in the underlying index. (but unlike traditional insurance, a buyer of protection does not need to have an underlying fundamental exposure).
- A seller of protection is “long” risk and a buyer is “short” risk.

J P Morgan

- In December 2011, the CIO was in the midst of an effort to reduce the Risk Weighted Assets (RWA) ascribed to the CIO portfolio because JPM Senior management had directed the CIO to do so to facilitate application of new BASEL II.5 requirements to JPM's overall business (due at 31 Dec 11)
- Initially, CIO tried to simply unwind some of the SCP short high-yield positions but found that this created losses
- CIO management then created conflicting trading objectives by re-focusing on profitability as well as reduction of RWA
- Traders added to the size of SCP and went long : mark-to-market losses increased
- Trading was suspended by CIO management on 23 Mar 12
- By 31 Mar 12, reported losses had reached \$718 million

J P Morgan

- During early April 2012, routine audit process for quarterly earnings involving PwC confirmed mark-to-market valuation of positions for loss calculation
- On 5 April 2012, Bloomberg and Wall St Journal ran stories about CIO trading & the “London Whale”
- Based upon information provided by CIO, JPM’s CEO described the issue as “a tempest in a teapot” during a 13 April JPM quarterly earnings call with analysts
- However, losses continued to rise so that by late April, senior JPM management called in a non-CIO risk management team to investigate
- This team concluded that SCP had much larger exposure to losses than previously reported

J P Morgan

- On 10 May CEO of JPM publicly disclosed that the trading strategy of SCP was “flawed, complex, poorly reviewed, poorly executed and poorly monitored”
- Losses in the 2nd quarter (up to 10 May) were estimated at some \$2 billion (in addition to the 1st quarter loss of some \$718 million) “with the possibility of future losses”
- A JPM Taskforce was then formed to investigate further
- The Taskforce found evidence that the 31 Mar 12 mark-to-market valuations underlying JPM’s 1st quarter earnings announcement were incorrect
- On 13 July, JPM announced a revision to lower its 1st quarter earnings by \$459 million and total losses incurred from SCP were \$5.8 billion as at 30 June

J P Morgan – JPM observations

- CIO management failed to :
 - understand, vet and monitor SCP trading
 - ensure that CIO risk and finance reporting functions were performing adequately (a new CIO CRO unfamiliar with SCP joined in Jan 2012)
 - appreciate the size and complexity of changes in the SCP early in 2012
 - ensure that adequate and accurate information was available to senior management about the SCP
 - accurately quantify the problem for a long period after it first arose
- JPM CEO should have given SCP more scrutiny, sooner
- JPM CFO failed to identify weaknesses in financial controls of SCP and failed to sufficiently question the SCPs RWA calculation and financial performance

J P Morgan – JPM Observations

- JPM Firm-wide risk management failed to identify shortcomings in risk management function of CIO (a new JPM CRO was appointed in January 2012)
- SCP risk limits were not granular enough – there were no limits on asset size, types, or risk factors within SCP
- Approval and implementation of a new CIO VaR model for the SCP in late January 2012 were seriously flawed and the model was not sufficiently reviewed or back-tested
- Both CIO and JPM (caused by CIO) breached their VaR limits several times between 16 and 26 January 2012. In essence, this was “corrected” by bringing the new SCP VaR model on-line on 27 January 2012.

J P Morgan – JPM Observations

- New VaR model was Excel based, complex, not readily auditable and not automated
- One spreadsheet error was identified on 10 April and corrected promptly (\$400 million loss)
- In May 2012, a further material error was discovered where a key volatility calculation divided by the sum of two parameters, rather than by their average as was intended
- This had the effect of halving volatility in key parts of the model and therefore significantly lowered VaR compared to what it should have been
- This, in turn, allowed much larger SCP positions to be taken
- VaR limits were not changed, even though new VaR model calculated a much lower VaR than the old model

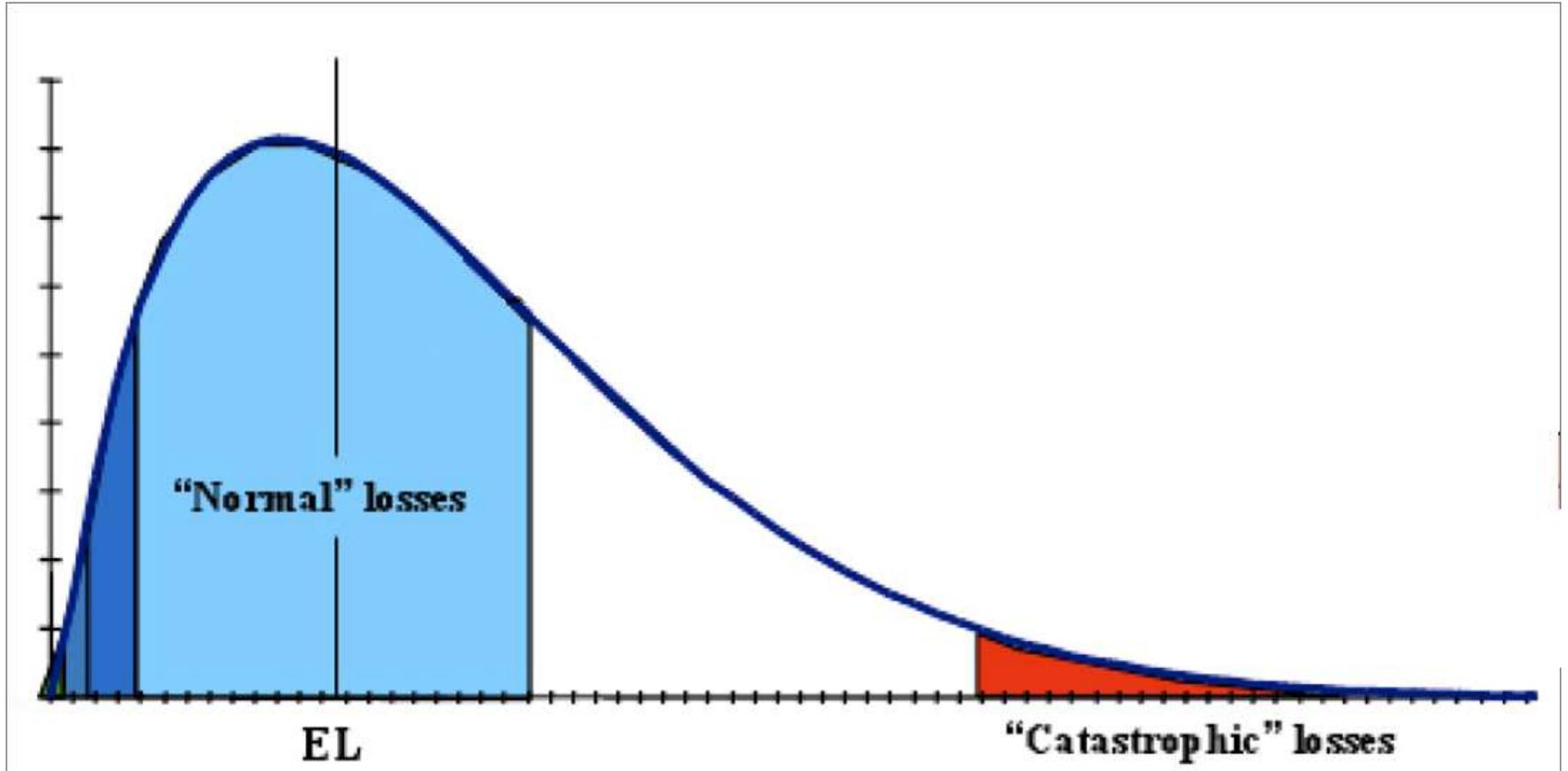
What do these events have in common ?

- They have all occurred recently and mostly after the onset of the GFC
- They all involve valuing greed or fear over integrity
- They all involve poor risk management / risk culture
- They reflect an attitude to risk taking that does not seem to have been reduced by large GFC losses
- In each case, the scale of the event is large with serious loss consequences for many stakeholders
- None of the events would have been prevented by the new BASEL III capital requirements
- Taken together with a lack of transparency on the real risks run by banks, they lead to a loss of investor trust in banks

Lessons learned ?

- Successful risk management needs to address risky behaviour in an organisation and needs to be about :
 - Setting values that drive behaviour within the organisation
 - Monitoring the way “bad news” travels within an organisation
 - Valuing “speaking up” when something is sub-optimal and preventing intimidation and bullying of those who do speak up
 - Setting up explicit measures of risk culture which are monitored
 - Using risk culture measures to financially reward / (penalise) good / (bad) managers as an integral part of bonus assessments
 - Being more transparent so investors and others can better understand risks that banks are running

“Value” at Risk



Some related issues

- “Normal” risk (closer to expected outcomes) is much more readily & easily quantified
- “Tail” risk (low frequency/high severity) is hard to accurately quantify – but VaR figures are often (slavishly) driven by it
- This can lead to over-reliance on VaR metrics
- VaR itself is often misleading – it tells you the predicted loss corresponding to a given probability, but does NOT tell you the amount of the expected loss for that probability or worse
- Imaginative “what if” stress and scenario testing are needed to supplement VaR metrics
- Cost pressures often lead to lack of quality / short cuts
- Management of tail risk events once they begin to unfold is also vital

In Conclusion

- Risk taking remains prevalent
- New BASEL III capital requirements are a necessary but not sufficient cure
- Behavioural risk is still not well understood or well managed
- Meaningful advances to measure and monitor risk culture and organisational behaviour will be key to achieving better outcomes in managing “tail” risks