A substantial fine , of US$ 150 million on Barclay's bank by the New York State Department of Financial Services (NYDFS) has given us a little glimpse into the future direction of bank misconduct and it is, to use the current catch cry, definitely 21st century.

Far from learning the lessons of the Forex Manipulation scandal, where Barclay's was fined over US$ 2.3 billion (yes billion) for manipulating the key FX benchmark used by pension funds around the world, traders have found new ways to defraud clients. One would have thought that such a severe slap would have caused Barclay's to change its behaviour. It did – it just moved the manipulation into cyberspace (where no one can hear you scam).

In the good old days (just last year), traders colluded with one another in Internet chat rooms to stiff clients by, for example, rejecting their perfectly good stop-loss orders. In the latest rip-off, Barclay's traders just used computers to do the stiffing. They programmed their computers to look at a stop loss order and if would incur a loss for Barclay's, then it was not executed.

And it was not just stop-loss orders. In an Orwellian fiddle named "Last Look", Barclay's computers would hold up trades for a few milliseconds and if the FX rates moved against Barclay's in the instant, the computer would reject them and send them bank to the client as a "NACK," which means "Not Acknowledged". Obviously, trades that benefited Barclay's were ACK'ed pretty sharpish. In telling emails on the scam, the rejected client trades were referred to as "toxic", which gives a good indication of where Barclay's head was at.

Again it was the email chain that caught the wrongdoers. When customers complained about the huge number of trades being rejected, Barclay's staff first stonewalled and then lied. Staff were told by management that under no circumstances were they to explain to customers how Last Look actually worked. They were told to say the trades were rejected because of "latency".

Latency, a word previously only used by IT propeller heads, has become the gold currency of High Frequency Trading (HFT). In this world, inhabited by ex-computer gamers, computers trade billions of dollars with each other every day, with little human intervention. Explaining how HFT works, Dr Marvin Wee reported that, in 2013, almost one third of all trades on the ASX were conducted between computers – it's almost certainly a lot more in 2015.

Could such a sophisticated fraud occur in Australia?

The short answer is yes it could, but we have no way of knowing whether it has occurred or not, or will in the future.

ASIC is the regulator responsible for “market conduct” and in 2013 published a report on HFT (and the ominous sounding Dark Liquidity) in which it stated basically – nothing to worry about here.

But to its credit, at the time ASIC was looking for evidence of the dangers of HFT to the markets, where badly programmed computers might run away, driving market prices down precipitously in what is called a flash crash . ASIC did not appear to looking for instances of intentional programming of anti-client behaviour, which of course is banned - but there again so was manipulation of the BBSW benchmark.

Fraud using HFT is insidious. It takes independent experts to look into the computer code in all HFT algorithms in all banks to detect potential manipulation by trading firms. Without regulatory pressure, there is no evidence that this is happening to any great extent.

And banks themselves are worried. Compliance and risk managers are now required by ASIC to consider what is called conduct risk, which has a very broad definition as “the risk of inappropriate, unethical or unlawful behaviour on the part of an organisation’s management or employees”. ASIC’s definition pretty well covers the hanky-panky that went on at Barclay’s. But how banks are supposed to manage that risk in this case is, to say the least, unclear.

Banking regulators were severely burnt in the GFC by reliance on computer models for calculating risk capital, so much so that the head of APRA, Wayne Byres, recently challenged regulatory orthodoxy
by posing the question “to model or not to model" concluding conclusively - sometimes.

It is time, given pressures that will inevitably come in the wake of yet another scandal involving banks defrauding customers, that regulators and bank executives begin to beef up their IT

resources to meet this 21st century challenge. And that does mean installing basketball hoops, it means training a whole new generation of forensic IT experts.

In this case, at least, the university sector appears to be leading the way.

Read more http://theconversation.com/21st-century-bank-fraud-demands-a-new-generation-of-it-experts-50967