Ravi Menon: Financial regulation – 20 years after the Global Financial Crisis

Keynote address by Mr Ravi Menon, Managing Director of the Monetary Authority of Singapore, at the Symposium on Asian Banking and Finance, Federal Reserve Bank of San Francisco, San Francisco, 25 June 2018.

* * *

Mr Mark Gould, Acting President, Federal Reserve Bank of San Francisco,

Ladies and gentlemen, friends and colleagues, good morning.

And welcome to the Symposium on Asian Banking and Finance 2028.

It was 13 years ago, in 2015, that the Federal Reserve Bank of San Francisco and the Monetary Authority of Singapore (MAS) began this collaborative journey of organising this Symposium.

- Let me, on behalf of MAS, thank Mark and his colleagues at the San Francisco Fed for the fruitful partnership and warm relationship over the years.

This Symposium began in 2007 to consider the lessons learned from the 1997 Asian Financial Crisis.

- Since then, we have lived through two other major crises – the Global Financial Crisis of 2008 and the Global Cyber Crisis of 2023.

Today, I would like to take stock of the evolution of financial regulation over the last 20 years, since the Global Financial Crisis. I think three broad themes characterise this journey:

- first, fixing the fault lines that led to the Global Financial Crisis;
- second, managing the risks posed by FinTech while harnessing its benefits;
- third, defending against systemic cyber risk.

Fixing the Fault Lines of the Global Financial Crisis

Let me begin with the regulatory and supervisory responses to the Global Financial Crisis. The advances over the last 20 years can be broken down into three broad phases.

The era of regulatory reform (2008 to 2016)

The first eight years following the Global Financial Crisis of 2008 saw the most wide-ranging set of reforms ever in the history of financial regulation. The destruction that the Global Financial Crisis had unleashed on our economies and societies galvanised action on an unprecedented scale.

The Global Financial Crisis revealed some deep fault lines in the financial system that had been masked by fortuitous growth.

- Many financial institutions had leveraged themselves to the hilt – some of them by as much as 40 dollars of debt to 1 dollar of equity – unthinkable these days.
- Many banks had severe mismatches in liquidity.
- An opaque OTC derivatives market led to rapid contagion when liquidity suddenly dried up.
- Moral hazard grew as some financial institutions were seen as too-big-to-fail.

The Financial Stability Board, or FSB, was strengthened and tasked to oversee reforms to address each of these vulnerabilities. The way the international regulatory community came together and forged a consensus on the necessary reforms was exemplary.

Between 2008 and 2016, the FSB, working closely with the Basel Committee, IOSCO, and other standard-setting bodies, put in place the basic building blocks for a new regulatory architecture that continues to serve us today.

- In banking, capital buffers were increased, liquidity requirements were introduced, and caps placed on leverage under a new Basel III accord.
- In the derivatives markets, requirements were put in place for trade reporting, central clearing, and margining.
- To tackle the too-big-to-fail problem, global systemically important financial institutions, or G-SIFIs, were identified and subjected to higher loss absorbency requirements, more intensive supervision, and resolution planning.

Implementation of the reforms – especially Basel III – progressed well, driven by a broad-based consensus on preventing a repeat of the Global Financial Crisis.

- The generous timelines for implementation allowed industry to adjust to the new regulatory landscape.
- It was only last year, in 2027, that we achieved full implementation of the final component of the Basel III reform package – the output floor.

Regulatory evaluation and adjustment (2017 to 2020)

During the second phase, from 2017 to 2020, the focus turned to evaluating the effects of the regulatory reforms.

- There was growing feedback that some reforms had unintended consequences, some reforms were at odds with others, and that the cumulative impact of the reforms had dampened economic growth.
- A series of reviews was undertaken during this period to assess both the effectiveness and effects of various reforms.

The reviews largely affirmed that the benefits of the reforms, in terms of reducing the risk of financial crisis and its consequent economic impact, far outweighed the costs.

- In fact, controlling for other factors, there was little evidence that the reforms resulted in any general deterioration in the availability or pricing of credit.

But the reviews did surface areas for improvement.

- They identified specific areas – like trade finance, infrastructure finance, SME finance and market liquidity – where the cumulative effects of various reforms had led to sub-optimal social outcomes.
- This led the way to carefully calibrated adjustments to regulations that eased the constraints in these areas without significantly increasing risk.
- The responsiveness and flexibility shown by regulators helped to sustain the broad-based political and industry consensus in favour of the post-crisis reforms.

Today, looking back from the vantage point of 2028, we can say with greater certainty that the post-crisis reforms have left us a financial system that is, on the whole, more robust and more resilient.

- Large banks are now stronger, more liquid, and less leveraged.
- Derivatives markets are safer and better collateralised.

The era of enhanced supervision (2021 onwards)

The third phase began from around the early 2020s, when the focus shifted away from rule-making to enhancing the supervision of financial institutions.

- The Global Financial Crisis was not just about gaps in regulation, it was also about gaps in risk management and supervisory oversight.
- Three developments in recent years added new impetus to the supervision agenda.

First, as the international activities of global banks increased and became more complex, regulators realised that effective supervision increasingly required much stronger cross-border co-operation and even co-ordination. The Basel Concordat II of 2024

- laid the foundation for more collaborative and meaningful supervisory colleges;
- strengthened the functioning of the crisis management groups; and
- set out more clearly the responsibilities of home and host supervisors.

Second, supervision extended beyond checking on financial institutions' risk management and internal controls to better understanding the risk culture of these organisations.

- Processes, controls, and limits can only go so far in restraining excessive risk-taking.
- Ultimately, it is people that take risks. And the incentive structure, governance practices, and value systems in financial institutions are what determine their attitude towards risk.

Regulators came together to establish common frameworks for what we now call culture and conduct supervision. This included sharing information on errant industry professionals to deter the problem of "rolling bad apples".

Supervisors began to use data analytics, sentiment assessments, and the tools of behavioural psychology to gain insights on the culture and conduct in financial institutions.

- These insights served as inputs to supervisory assessments of the risk culture in financial institutions and, where necessary, pre-emptive interventions.

Third, the active integration of technology into the supervisory process – what we now call SupTech – began to dramatically enhance supervisory effectiveness by the mid-2020s.

- Data analytics finally solved the long-standing challenge that banks had in aggregating credit and market exposures across various businesses and geographies.
- This enabled banks to derive a consolidated risk profile in real-time.
- And the integration of RegTech and SupTech allowed data from financial institutions to flow directly into regulators' data bases in machine-readable formats through Application Programming Interfaces or APIs.

Supervisory officers, who used to spend long hours poring over spreadsheets and reports – cutting, pasting, and computing – began to use automated surveillance dash boards.

- They are able to track on a daily basis the consolidated exposures, credit quality, value-at-risk and other indicators of the banks under their purview.
- They are able to carry out stress tests and simulations not only of individual banks but also network analysis of risk transference across the financial system.

Compared to just ten years ago, technology has enabled supervision to become much sharper and surveillance of systemic stability more rigorous.

Managing the Risks Posed by FinTech while Harnessing its Benefits

The second big theme in financial regulation over the last 20 years is the rise of FinTech.

Technology has always featured in financial services. But from about 2015 onwards, there was an explosion in the application of various technologies in financial services – by both regulated entities and unregulated FinTech firms offering niche financial products.

FinTech transformed the way financial services were produced, distributed, and consumed.

- It has brought significant benefits to consumers, financial institutions, and the economy at large.
- It has helped to reduce costs, manage risks better, create new business opportunities, and improve people's lives.

But like all good things, FinTech brought in its wake new risks and new challenges for regulators. The story of FinTech regulation is still unfolding but let me highlight three areas where good progress has been made in the last 10 years:

- setting standards for distributed ledgers;
- making cloud computing services safer; and
- dealing with artificial intelligence.

Setting standards for distributed ledgers

Experiments in applying distributed ledger technology to financial services began about 15 years ago and gathered pace from about 2018 onwards. The early days were characterised by both hype and fear.

- Popular imagination and regulatory concerns were focused on so-called crypto currencies or assets – essentially crypto tokens which assumed a life of their own as means of payments or investment assets outside the distributed ledger.
- But the euphoria did not last long. Crypto tokens failed to achieve scale as more people realised that they did not have the properties of either currencies or assets.
- Today, crypto tokens are confined to specific purposes and limited ecosystems.

But after several false starts and failed use cases, the underlying distributed ledger technology or DLT started making significant inroads in the financial industry.

- Essentially, DLT made financial transactions and processes more efficient, more transparent, less risky, less costly.
- The three areas that saw the biggest transformations were in compliance, trade finance verification, and cross-border payments.

As DLT systems became more pervasive, they began to assume properties of critical infrastructure with systemic implications.

- There were information security-related risks as well as operational risks associated with interoperability across multiple platforms.
- While strong cryptography is a feature of DLT systems, they are not immune to cyber-attacks through the widely distributed network of participants.

- And old-fashioned risks like not having enough liquidity to settle transactions can potentially lead to gridlocks in DLT systems which could, in turn, cause systemic risks.

The trigger for a co-ordinated regulatory response to DLT came in the cross-border payments space.

- In 2020, the Bank of Canada and Monetary Authority of Singapore successfully piloted a cross-border DLT-based system that achieved almost real-time fixed income securities trading and settlement.
- Under the Global Payments Accord of 2024, central banks agreed to upgrade their real-time gross settlement systems to a DLT-inspired infrastructure with a view to connect these systems for safer, faster, and more efficient cross-border payments and settlements.
- This called for internationally accepted standards for DLT-based payment systems.

The FSB and standard-setting bodies worked closely with the newly-formed International Organisation for Distributed Ledger Standards to design a supervisory framework for DLT.

- DLT networks that performed key market functions like clearing and trade reporting were required to meet specified standards for settlement finality and the security of digital asset custody.

Making cloud computing services safer

From about 2015, financial institutions increasingly began to use the cloud.

- With cloud computing, financial institutions could efficiently integrate customer data across platforms to enable sharper consumer insights.
- The cloud provided scalable storage solutions to meet the real-time demands of trading and analytics processes.
- Some banks have even moved their core banking systems into the cloud to reap the benefits of its scalability and resilience.

Cloud computing has considerably enhanced risk management. Risk assessments are now more comprehensive, more granular, and more real-time.

But the cloud has also introduced new risks. The risks are not so much in the technology of cloud computing per se but in the business and operating models of cloud services.

- Cloud services are essentially a utility provided by specialist third-party providers.
- And as with any third-party service provider, there are outsourcing risks associated with these cloud service providers or CSPs.

But with cloud computing, these outsourcing risks are much larger, given how much of a financial institution’s data and processing functions rely on CSPs.

- Financial institutions have less knowledge, let alone control, of where their data are stored in a cloud computing infrastructure spanning several different jurisdictions.
- Data breach or loss might occur due to a natural disaster, targeted attack, or poor security processes at the CSPs.

The outsourcing risk is compounded by concentration risk.

- The top 4 CSPs in the world had a market share of 80% last year.
- About 25% of the core banking systems of global systemically important banks or G-SIBs is

now residing on the cloud.

- A large supplier of cloud services can potentially become a single point of failure when many financial institutions rely on them.

The regulatory response to cloud computing has taken two forms.

First, regulators around the world have issued regulations or guidance on the management of outsourcing risks pertaining to cloud services.

- The Monetary Authority of Singapore and the UK Financial Conduct Authority were among the first regulators to do so, as early as 2013.

Second, the jurisdictions where these CSPs operate from have begun to exercise regulatory oversight over them.

- In the US, the Cloud Services Utility Agency, or CSUA, was formed in 2024 with the mandate of regulating CSPs, working closely with the US Federal Reserve System.
- I am pleased that the Federal Reserve Bank of San Francisco has been designated as the lead regulatory co-ordinator with the CSUA, as two of the four globally dominant CSPs are based in California.

Dealing with artificial intelligence

The use of AI has swept across the financial services sector in recent years.

- Banks are benefitting from AI through better customer insights, increased productivity, and cost savings.
- AI applications range from customised financial services to enhanced risk management and regulatory compliance.

But the growing application of AI has also introduced new risks and challenges for regulators.

Foremost are concerns about market disruption and financial instability caused by runaway AI trading algorithms.

- The global flash crash of August 2022 demonstrated the contagion risks that multiple AI trading programmes “learning” from one another can precipitate.
- When an AI trading algorithm went amok and caused the failure of US hedge fund Smart Money, AI traders across America, Europe, and Asia went into a massive risk-off mode, causing turbulence not only in equities but also fixed income, commodity, and currency markets.
- Herd behaviour has always been a characteristic of financial markets. But herds of robots have proven to be far more deadly than herds of humans.

The International Organisation of Securities Commissions (IOSCO) has since mandated that exchanges have in place mechanisms to manage extreme volatility.

- And securities regulators have themselves started to use AI – to provide early warning of potentially disruptive AI-based trading patterns and trigger appropriate circuit-breakers.

But more generally, the increased use of AI by financial institutions has created the risk of “black boxes” in decision-making.

- Boards and senior management of financial institutions are struggling to validate AI-based models which use continuous learning and adaptation as distinct from fixed parameters and

historical back-testing.

The application of AI in financial services has also created issues of financial exclusion which regulators cannot ignore.

- Regulators have begun to detect cases where AI-based decision-making has led to systematic exclusion of certain demographics.
- When an AI tool finds an empirical basis for discriminating by a combination of variables such as gender, ethnicity, religion, and nationality, say for a loan or insurance decision, how much of that empiricism is grounded in reality and how much of it is due to unobserved biases in society that the AI is learning from?
- And even if such discrimination is backed by empirical unbiased data, is that a socially acceptable outcome?

Regulators in many jurisdictions have been engaging the industry as well as the broader society on developing guidance on the responsible and ethical use of AI and data analytics by financial institutions.

Defending Against Systemic Cyber Risk

The third theme that stands out in the history of financial regulation over the last two decades is cyber security.

- But it was only after the Global Cyber Crisis of 2023 that cyber risk management has moved to front and centre of the international regulatory agenda.

The Global Cyber Crisis laid bare our cyber vulnerabilities.

- A highly skilled and well-resourced group of hackers used AI-enabled malware to infiltrate banks across the world, subvert detection, and siphon monies.
- Over a span of just 6 weeks, a total of US$45 billion was stolen from over 500 banks, leading to loss of public confidence and bank runs in several jurisdictions.
- Only 8% of the stolen funds has ever been recovered.

The failure of Algor Bank at the height of the Global Cyber Crisis demonstrated both the high points and low points in financial regulation.

Algor Bank was successfully resolved with minimal disruption.

- Thanks to efforts by the FSB after the Global Financial Crisis, the major jurisdictions that Algor Bank operated in had robust resolution regimes.
- With a clear resolution plan formulated, tested and discussed at the bank's annual Resolution College prior to the crisis, home and host regulators were able to resolve Algor Bank in a smooth and timely manner.

But the fact that a cyber attack could bring down the 20th largest bank in the world with a Tier 1 capital adequacy ratio of 16% revealed significant gaps in the global regulatory regime for technology risk.

- It was ironic that in an industry where there were detailed internationally accepted standards for capital, liquidity, and a range of prudential norms, there were no standards for cyber risk management.

The FSB and standard-setting bodies swung into action and in 2025 produced a two-track set of reforms to deal with cyber risk, which is essentially borderless.

First, the FSB's Cyber Security Standards, building on its Cyber Lexicon of 2018, established a minimum level of cyber hygiene for internationally active financial institutions.

- They set out harmonised standards for authentication, implementation of cryptography, intrusion detection, and incident reporting.

Higher standards were set for G-SIFIs.

- G-SIFIs were required to put in place 24/7 cyber surveillance of all Internet-facing systems, undergo annual cyber vulnerability assessments by internationally certified cyber specialists, and carry out military-grade penetration tests.

Second, the Basel Committee and IOSCO developed core principles and practice guides for prompt information sharing on cyber incidents and cyber threat intelligence among banks and securities firms respectively.

- National laws were amended, where necessary, to facilitate information sharing across these financial institutions without incurring legal liability.

Global platforms were put in place to facilitate information sharing among central banks and regulators to counter cross-border cyber threats of the kind that triggered the Global Cyber Crisis.

- Through these platforms, financial regulators are able to quickly disseminate useful cyber threat information to banks and securities firms so that they can take pre-emptive measures.
- These platforms built on the success of the earlier Central Banks, Regulators and Supervisory entities or CERES platform of 2018 which enabled effective sharing of actionable cyber threat information.

But the enemy has not been lying still.

- Hackers are now employing more advanced quantum computing technologies, and a number of weaker encryption solutions used by financial institutions have been compromised.
- Cybersecurity continues to be a cat-and-mouse game. There is no room for complacency.

Conclusion

Let me conclude.

The financial system today is more robust and resilient than it was 20 years ago.

- The wide-ranging regulatory reforms following the Global Financial Crisis have stood us in good stead.
- There is broad consensus across industry and the regulatory community on the value of sound regulation and risk management.

But the financial landscape has also transformed dramatically over these two decades.

- The rise of FinTech has changed the face of financial services.
- Technology has helped us reduce some risks and better manage others, but it has also introduced new risks and vulnerabilities.
- The regulator's job is never done.

And while we have gotten better at managing traditional risks such as credit and market risk,

cyber risk has now moved to the front of the regulatory agenda.

But while the landscape has evolved and the nature of threats to financial stability has changed, the core principles of sound regulation remain evergreen.

- The goal is to keep the financial system stable and maintain public confidence and trust in the financial sector.
- And to do this in a way that allows the financial sector to innovate and grow, and serve the needs of the economy and society.
- That means taking a proportionate approach to risk, so that we can achieve resilience with efficiency, stability with growth, safety with innovation.

Thank you.

Everything said here about the future is pure imagination; it is neither a forecast nor a recommendation, by me or the Monetary Authority of Singapore. My intention is merely to paint a plausible scenario for the future of financial regulation, as food for thought for this Symposium. In all likelihood, the Symposium of 2028 will find my account lacking in imagination or realism or both. The truth will be stranger than fiction.