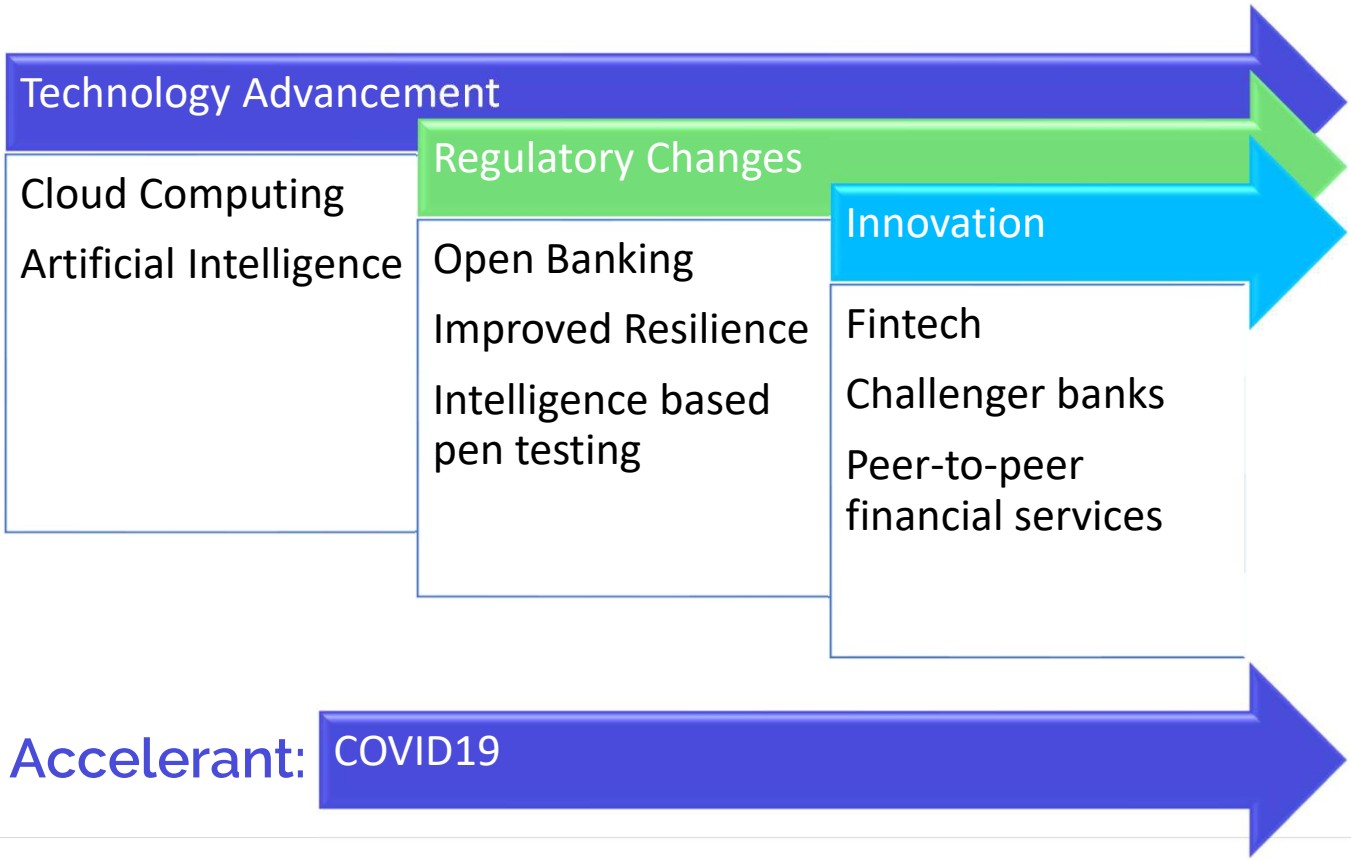
FS-ISAC

Financial Services in a changing world

Information Security Summit (IS Summit)

Introduction

Drivers for Change



Impact of COVID19

- Huge changes to working practices driving remote working and digitisation.
- 75% of FS-ISAC members are reporting making significant changes to their cyber programs as a result of the crisis.
- 3% reported changes needed to digital banking tools, suggesting they were fit for purpose.
- 11% were more concerned than normal by 3rd party risk.
- 46% are expecting to see more investment in cyber post crisis.

Source: FS-ISAC member poll

Technological Advances

Cloud Computing 1/2

Opportunities:

- Cost reduction
- Rapid deployment of new services
- Modernise & and standardise busines processes

Obstacles:

- Concerns over control and security of data
- Compliance with local and global regulation
- Integration with existing legacy architecture
- Performance and resilience
- Vendor lock in

Source: Deloitte Global Outsourcing Survey 2018

Cloud Computing 2/2

- Cloud adoption in financial services is picking up speed. 88% of FS-ISAC members in the US now have some services outsourced in the cloud.
- Cloud vendors now offer solutions to most obstacles:
  - In country and private hosting options are available
  - Secure hosting services as or more secure than on prem
  - Regulators are catching up with and starting to accept cloud
  - Open source platforms allow easy portability
  - Built in resiliency with advanced replication capabilities
  - Rapid deployment ability to scale capacity up or down quickly
  - Business friendly connected data sets, improved analytics, automation.
- This makes cloud adoption mandatory for financial services firms that wish to stay competitive.

Artificial Intelligence

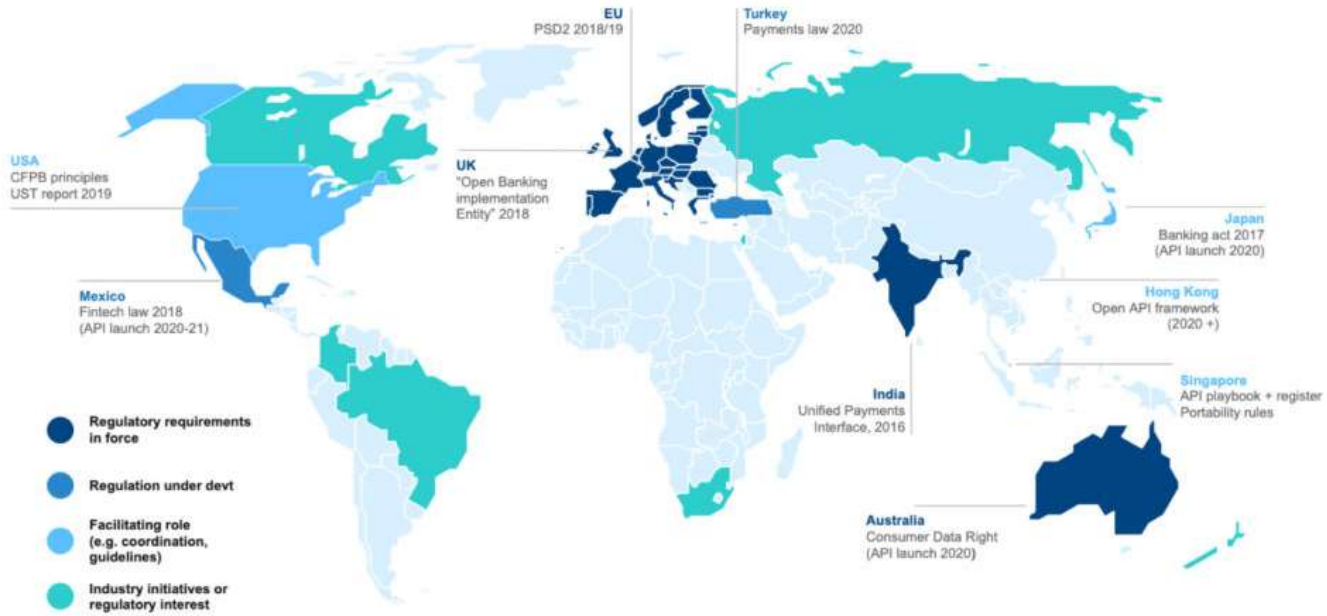
- AI has huge business benefits in Finance:
  - Front office: conversational banking, biometrics, personalised insights.
  - Middle office: anti fraud, risk reduction, AML & KYC.
  - Back office: credit underwriting, smart contracts (blockchain).
- In Cyber Security AI can be used by both defenders and by attackers:
  - **Defenders:** help to improve controls, primarily through automation, to secure the Confidentiality, Integrity and Availability of data while also posing challenges as new business processes to exploit AI must in turn be protected.
  - **Attackers:** leverage AI automation to conduct attacks that were not previously possible. Substantial cloud and AI adoption means that attacks that are effective against them to be effective against many firms.

Source: Oliver Wyman Artificial Intelligence Applications in Financial Services

Regulatory Changes

Open Banking 1/2

Open Banking refers to the liberation of customer data and accounts to 3rd parties vi APIs.



Open Banking 2/2

- May be limited controls regarding **which firms can act** as third parties.
- Clear rules on **liability and dispute resolution** are missing which would ensure that if a problem does occur it's clear how the different entities involved should resolve it.
- Not all frameworks have been designed with their **sustainability** in mind: for example with PSD2 in Europe, any charging for API access is prohibited.

Improved Resilience

- We have recently seen many new papers on operational resilience from Financial Stability Board, Bank of International Settlements, Bank of England, etc.
- Key point is a move from thinking about operational risk to operational resilience.
- To achieve operational resilience:
  i. Identify the important business services provided by a firm
  ii. Set impact tolerances for disruption including time limits to resume the delivery of services
  iii. Invest to build resilience so as to stay within these tolerances in severe but plausible scenarios.
- Operational risk is a tool to help deliver operational resilience.

Resilience During COVID

- COVID forced focus on maintaining the delivery of important business services with reduced staff and very large increases in remote working.
  - More successful than expected, largely due to recent technical capabilities.
  - Increase in remote working placed pressure on IT systems: required capacity increases including sourcing and configuring new IT equipment quickly and in large numbers.
  - At the same time firms had to deal with increasing demands for certain services (such as new loan requests or mortgage payment holidays).
- We were lucky:
  - Slow - could see it coming; response time was measured in days & weeks. We had time to think, prepare and implement.
  - Prolonged – giving us time to understand and adapt to changing circumstances.
  - Symmetric – threat has been broadly equal to everyone, everywhere, at the same time.
- Fast, short-lived and asymmetric is much worse. Cyber, complex operational failures or key third party failures are examples.

Threat Intelligence Based Pen Testing

Current Examples: CBEST (UK), TIBER (EU), iCast (HK)

	Vulnerability Assesment	Pen Testing	Red Teaming	Threat Led Pen Testing
Objective	Broad scan for vulnerabilities	Find vulnerabilities	Test detective and reactive controls	Threat led red teaming
Techniques	Automated	Specialized Team	Specialists emulating threat actors	Simulate real life threats
Scope	Single System	Specific Application	Whole entity	Whole entity
Costs	Low	Medium	High to very high	High to very high

Innovation

History of Banking

- ~2000 BC – Asian merchants lent money to farmers
- ~0 – Roman Empire money lending and minting of coins occurred in temples.
- 1100 – Knights Templar run early European banks
- 1397 - Medici merchant bank in renaissance Italy
- 1565 – London Royal Exchange (goods exchange)
- 1602 – Amsterdam Stock Exchange (venue for FS-ISAC summit 2018)
- 1694 – Bank of England founded
- 1700 – Chinese draft banks (Piaohao) and native banks (Qianzhuang)
- 1720 – South Sea Bubble caused a European financial crisis
- 1897 – Imperial Bank of China opened

Fintech Definition

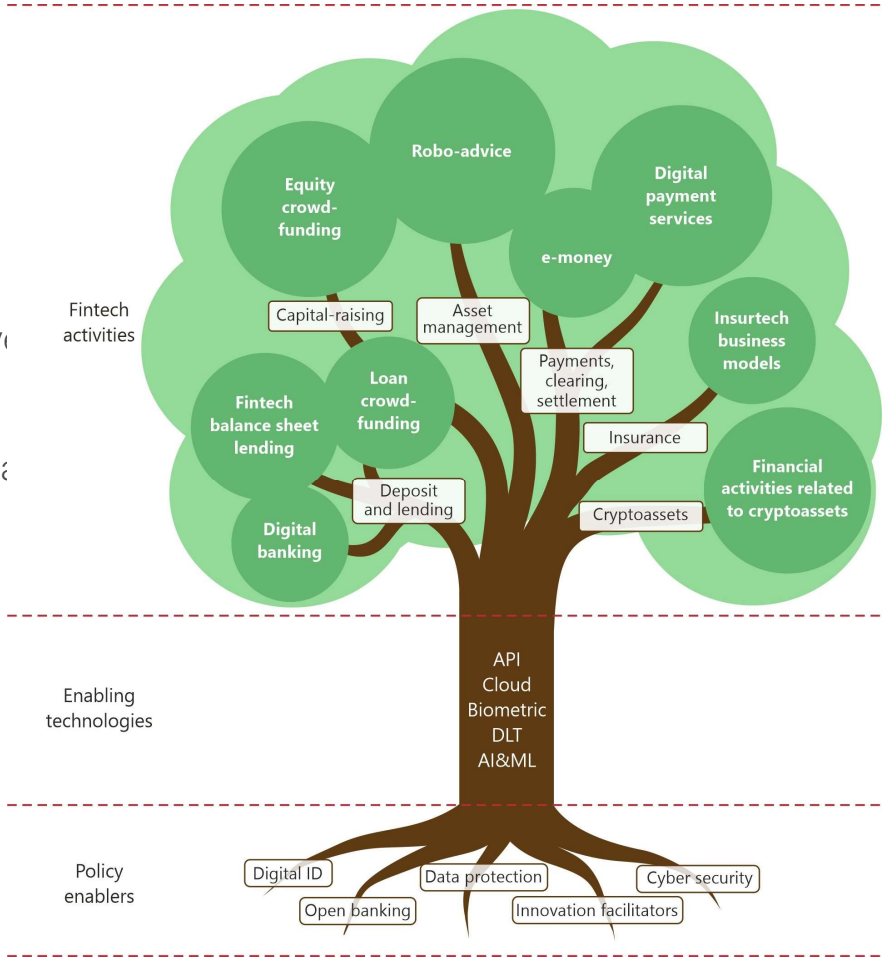
Fintech is not a business category in it's own right – it is a new way of doing old business.

Definition: *technologically enabled financial innovation that could result in new business models, applications, processes or products with an associated material effect on financial markets and institutions and the provision of financial services.*

Fintech

6 Categories:

i. deposits and lending
ii. capital-raising and alternativ sources of funding
iii. asset management, trading a related services
iv. payments, clearing and settlement services
v. insurance
vi. cryptoassets



Source: FSI Insights on policy implementation No 23

Challenger Banks

- Small, recently created retail banks that compete directly with longer established banks.
- Typically use modern financial technology practices and online only operations to avoid costs and complexities of traditional banking.
- European examples of Challenger banks include Revolut, N26, Starling, Monzo.

Peer to Peer financial services

Use modern technology to bring parties together for financial transactions, for example:

- Loans – for e.g. Zopa in the UK and Prosper in the US.
- Underwriting - mobile, on-demand, usage-based or technology-enabled peer-to –peer insurance – e.g. Guevara (UK), Lemonade (US), Friendsurance (Germany)
- Payments – for example peer to peer money transfers with Transferwise.

Thank you

For more information about FS-ISAC Contact:

Chris Wong: cwong@fsisac.com

To contact me:

Ray Irving rirving@fsisac.com

