CHALLENGES FOR ISLAMIC BANKS IN DIGITAL ERA

Dr. Salman Ahmed Shaikh, Assistant Professor of Finance

Presentation Outline

- Overview of Islamic Banking Growth
- Cybersecurity and Banks
- Technology Upgradation Risks in Digital Era
- Operational Risks in Technology Upgradation
- Shari'ah Non-Compliance Risk in Digital Space
- Commercial Risks Triggered by Fintech
- Coping up with Commercial Risks in Digital Era
- Questions & Answers

Overview of Islamic Finance

Year	Islamic Banking Assets ($Billion)	Islamic Finance Assets ($Billion)
2012	1305	1746
2013	1565	2050
2014	1445	1965
2015	1604	2190
2016	1675	2290
2017	1721	2438
2023	2441 (Projected)	3809 (Projected)

Growth in Islamic Banking and Finance (212-2017)
Source: Thomson Reuters Global Islamic Finance Report 2018

Overview of Islamic Finance

Year	Islamic Funds ($ Billion)	Sukuk ($ Billion)
2012	46	260
2013	54	284
2014	59	299
2015	66	342
2016	91	345
2017	110	426
2023	325	783

Growth in Islamic Fund Assets
Source: Thomson Reuters Global Islamic Finance Report 2018

Overview of Islamic Finance

- In global Islamic finance assets, the share of *Takaful* is 2% *(Source: Reuters, GIFR 2018)*.

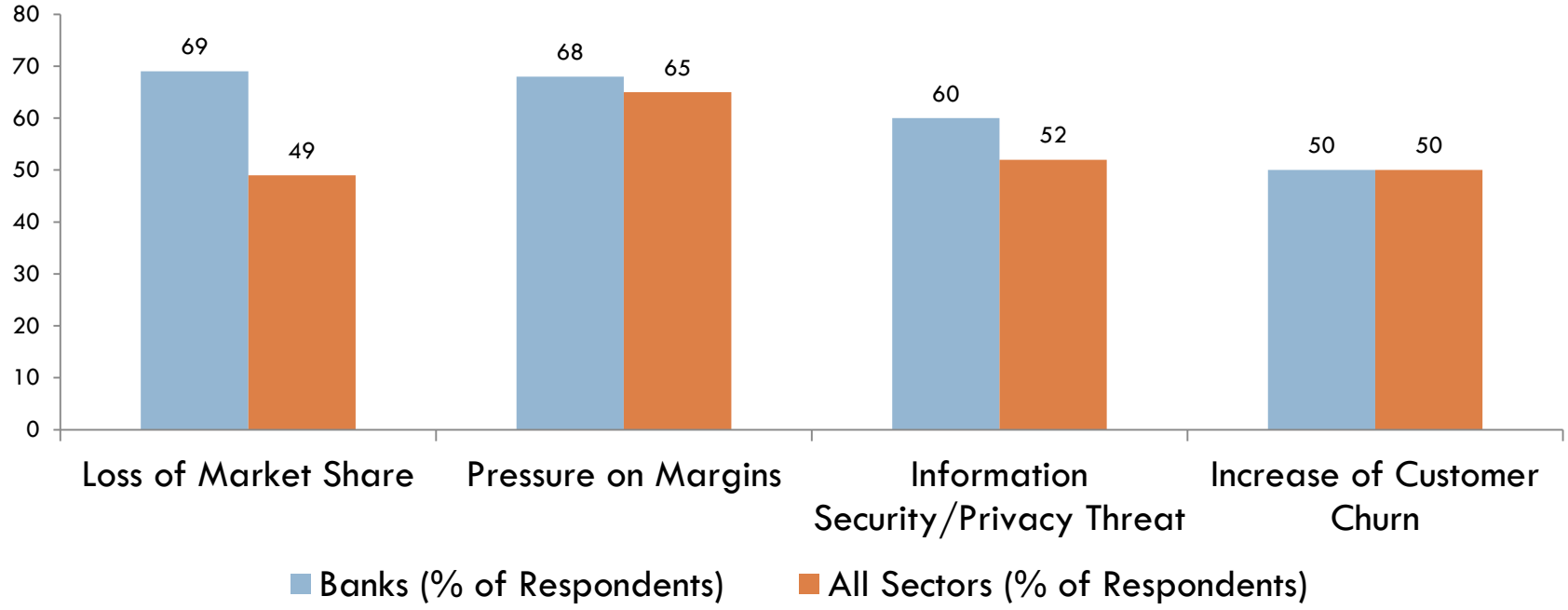
- With a CAGR of 6%, *Takaful* assets have grown from $ 31 billion to $ 46 billion in 2017 as compared to 2012 *(Source: Reuters, GIFR 2018)*.

- In 47 countries, there are 324 *Takaful* operators operating globally *(Source: Reuters, GIFR 2018)*.

Challenges Faced by Islamic Banks in Digital Era

- Common Technology Risks + Some Additional Risks.
- Operational Risks in Digital Transformation of Operations and Service Delivery.
- Cybersecurity Threats and Risk.
- Shari'ah Non-Compliance Risk.
- Commercial Displacement Risk.

Challenges Posed by Technology



Source: PwC 2016 Survey on Fintech Challenges

Significance of Cyber Crimes for Banks

- Accenture and the Ponemon Institute in its report "Cost of Cyber Crime Study," found that:

"The average cost of cybercrime for financial services companies globally has increased by more than 40 percent over the past three years, from $12.97 million USD per firm in 2014 to $18.28 million USD in 2017 — significantly higher than the average cost of $11.7 million USD per firm across all industries included in the study. The analysis focuses on the direct costs of the incidents and does not include the longer-term costs of remediation."

Significance of Cyber Crimes for Banks

- A Forbes report highlights several statistics regarding banks and cybercrime:
  - Cybercrime costs banks more to recover from than businesses in any other industry.
  - The rate of breaches in the financial sector has increased by 300 percent over the past five years.
  - Banks are breached by hackers 300 times more frequently than firms in other industries.
  - Cybercrimes cost banks over $1 trillion each year.

Cybersecurity Threats in Digital Space

- Leakage of Private Confidential Information. E.g.
  - Debit Card Details.
  - Credit Card Details.
  - Personal Identification Information.
  - Transaction Activities.
  - Account Balance.
- Unauthorized Access to Accounts.
- Unauthorized Debits.

Bank Theft Examples in 2019 Alone

- **Indian ATMs Targeted with ATMDtrack Malware**
- On September 23, security researchers reported that North Korean hackers had developed and inserted malware to steal payment information from Indian ATMs and banking institutions.

- **ECB BIRD Site Data Breach**
- On September 16, the European Central Bank (ECB) shut down its Banks' Integrated Reporting Dictionary (BIRD) site after routine maintenance uncovered a cyberattack compromising the information of the site's newsletter subscribers.

- **Himalayan ATM Heist**
- On September 2, Nepalese police arrested five Chinese nationals in connection with cyberattacks that cost Nepalese banks more than 35 million rupees (over $300,000).

Bank Theft Examples in 2019 Alone

- **Binance Ransomware**
- On August 6, Malta-based cryptocurrency exchange Binance became the victim of ransomware when attackers demanded 300 bitcoin (around $3.5 million at the time) in exchange for a Know Your Customer (KYC) database containing the personal information of around 10,000 users.

- **Capital One Data Breach**
- On July 29, Capital One announced that it had suffered a data breach compromising the credit card applications of around 100 million individuals after a software engineer hacked into a cloud-based server.

- **Banco Pan Data Breach**
- On July 25, security researchers found a file containing 250GB of personal and financial information, mainly tied to Brazilian financial institution Banco Pan, exposed online.

Bank Theft Examples in 2019 Alone

- **Jana Bank Data Breach**
- On July 23, a security researcher reported that Jana Bank, an Indian small finance bank, left exposed a database containing information on millions of financial transactions.

- **Remixpoint Inc. Crypto Theft**
- On July 12, Remixpoint, a Japanese cryptocurrency exchange, halted services after it discovered the theft of $32 million in digital currencies.

- **Crypto Exchange Theft**
- On June 25, Europol, British law enforcement, and Dutch law enforcement officials arrested six individuals for cryptocurrency theft amounting to €24 million (over $26 million).

Bank Theft Examples in 2019 Alone

- **Bangladesh Switch System Cyberattack**
- In June 2019, at least three private Bangladeshi banks were compromised by major cyberattacks, with one, Dutch Bangla Bank Limited (DBBL), losing as much as TK 25 crore (around $3 million).

- **First American Financial Corp.**
- On May 24, First American Financial Corp. suffered a data breach compromising around 885 million files related to mortgage deeds.

- **FirstBank Breach**
- In May 2019, a Colorado bank suffered an external security incident resulting in the cancellation and redistribution of customer debit cards.

Bank Theft Examples in 2019 Alone

- **Retefe Malware Resurfaces in Germany and Switzerland**
- In May, U.S. security company Proofpoint reported the return of the Retefe banking Trojan in Germany and Switzerland.

- **Romanian ATM Skimmer Gang Arrested in Mexico**
- On March 31, Mexican law enforcement arrested two members of a Romanian cyber-criminal group allegedly behind an ATM skimming operation in Mexico.

- **Royal Bank of Scotland Security Flaw**
- In early 2019, the Royal Bank of Scotland's (RBS) customer accounts were exposed to a security flaw after introducing a new customer security service.

- **Ursnif Malware Attack on Japanese Banks**
- The Ursnif banking Trojan, which was discovered in 2007, was repurposed in a campaign targeting Japanese banks that began in 2016.

Bank Theft Examples in 2019 Alone

- **Bank of Valletta**
- On February 13, the Bank of Valletta (BOV), Malta's largest and oldest bank, shut down operations after an attempted theft of €13 million.

- **U.S. Credit Union Spear-Phishing**
- On February 8, Multiple credit unions in the United States were hit by spear-phishing emails impersonating compliance officers from other credit unions.

Bank Theft Examples in 2019 Alone

- **Metro Bank 2FA Breach**
- On February 02, UK-based Metro Bank became the first major bank to suffer from a new type of cyber intrusion that intercepts text messages with two-factor authentication codes used to verify various customer transactions.

- **Chile ATM Attack**
- On January 10, hackers infiltrated Chile's ATM interbank network, Redbanc, after tricking an employee into downloading a malicious program during a fake job interview over Skype.

Technology Upgradation Risk in Digital Era

- Need for Customized Upgradation to Incorporate Islamic Product Structures.
- Need for Customized Nomenclature to Ensure Distinctness from Conventional Banks. E.g. Avoiding terms like 'Interest', 'Loan' in ERPs etc.
- Need to Comply with SOPs and Protocols in Islamic Product Structures.
- Need for Ensuring Platform Security. E.g.
  - Website for Online Banking.
  - App for Mobile Banking.

Operational Risks in Technology Upgradation

- Need for Updating SOPs for Monitoring. E.g. Know Your Customer (KYC), Biometric Verifications.
- Installing Multiple Security Checkpoints. E.g. Thumb Impression, Face Recognition, Security Codes, Personal Identification Number (PIN), One-Time-Password (OTP), QR Codes etc.
- Staff Training for
  - What They Can and Can Not Ask.
  - What They Should Ask to Ascertain Proper Identification.
  - What They Shall Not Reveal About Customers.

Shari'ah Non-Compliance Risk in Digital Space

- Impermissible Use of Funds in Shari'ah Non-Compliant Services. E.g. Non-Halal Restaurants.
- Charging Customers Prematurely Before the Asset Delivery in Islamic Lease.
- Need for Combining Physical Monitoring with Automated Processes.
- ERPs and Electronic Accounting Software Need to Incorporate Islamic Product Structures, Nomenclature & Regulations.

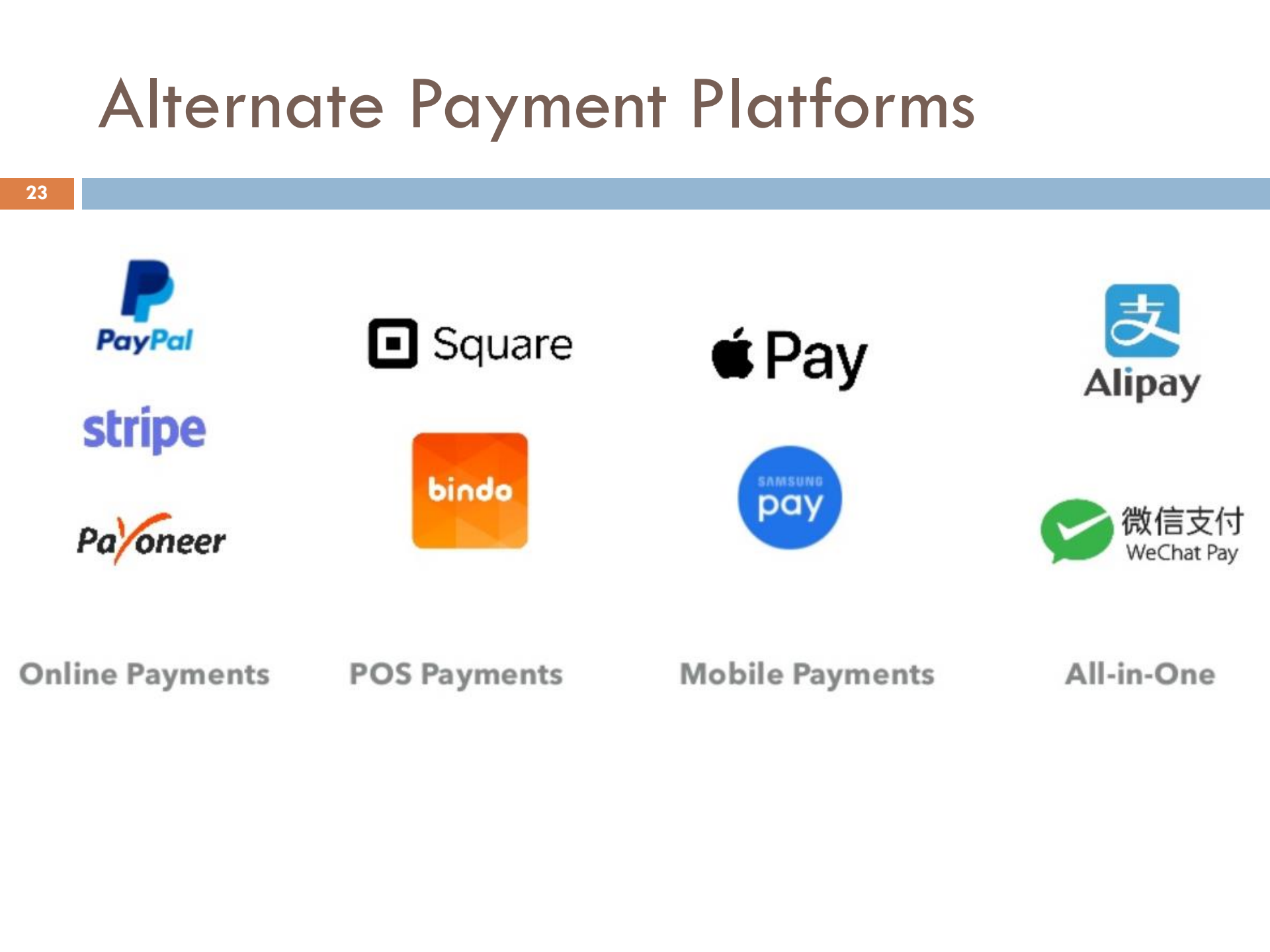
Commercial Risks Triggered by Fintech

- Less Loyalty and Switching Costs.
- Banking is Necessary, But Banks Are Not.
- Alternate Banking Models of Future
  - Bank-as-a-platform (BaaP).
  - Bank-as-a-service (BaaS) are Models of Future.
- PWC Fintech Survey 2016 Reveals
  - 83% survey participants believe that Fintech will disrupt some part of business of traditional banks.
  - 73% agree that consumer banking will be disrupted.
  - 55% agree that fund transfer and payment will be disrupted.

Commercial Risks Triggered by Fintech

- Lower Barriers to Entry in Payments Business.
- New Generation of Customers are Increasingly Targeted and Won over in Digital Space.
- Competitive Payment Networks. E.g.
  - PayPal,
  - E-Wallets,
  - Cryptocurrencies.

Alternate Payment Platforms



Commercial Risks Triggered by Fintech

- Non-Banking Financial Intermediation. E.g.
  - Crowdfunding.
  - P2P Lending.
- Money Laundering to Offshore Regions.
- Funds Transfer for Criminal Intent. E.g.
  - Terrorism Financing.

Coping up with Commercial Risks in Digital Era

- Invest more in technology infrastructure than physical infrastructure. E.g.
  - Cloud Computing.
  - Artificial Intelligence.
  - Blockchain.
  - Mobile Apps.
- Ensuring user friendliness in User Interface (UI) as well as ensuring multi-layered security protocols.
- Cross selling other products. E.g.
  - InsureTech.
  - InvestTech.

Coping up with Commercial Risks in Digital Era

- Use Interactive Digital Communication. E.g.
  - Chatbots.
  - Robo Advisors.
- Providing one-stop operation to facilitate payments, investments and availing services like credit and insurance.
- Creating network externalities to engage and retain customers.
- Need for active bank-vendor relationships to offer exclusive discounts to retain customers.

Questions and Answers