IT Risk: Cybersecurity

Agenda – Purpose of Presentation

- Define cybersecurity
- Describe the challenges unique to cyber risk
- Discuss how financial institutions have responded to cyber risk
- Describe supervisory tools used for this risk
- Discuss approaches to supervising cyber

Ground Rules for Cybersecurity Discussion

Cybersecurity…

does not recognize borders, so neither should your comments and questions.

is a dynamic risk, so think outside the box in terms of supervisory approach.

is a pervasive business risk, so consider our discussions as a safety and soundness challenge where technical skills are not required.

risk management places great importance on information sharing, so share for the betterment of all.

What is Cybersecurity?

How would you define Cybersecurity?

- Is there an organization /agency whose definition you utilize?
- What immediately comes to mind when you hear the term?
- What connotations does it carry within your country?

1. identification
2. information security → 3. operation & data security
4. protection, recovery.

What is Cybersecurity?

A broad concept for which there is no consensus definition…

Strategies, policies and standards encompassing the full range of threat reduction, vulnerability reduction, deterrence, international engagement, incident response, resilience, and recovery activities and policies regarding the security of (an FMI's) operations. – *Bank for International Settlements*

The collection of tools, policies, security concepts, security safeguards, guidelines, risk management approaches, actions, training, best practices, assurance and technologies that can be used to protect the cyber environment and organization and user's assets – *International Telecommunications Union*

The protection of information assets by addressing threats to information processed, stored, and transported by internetworked information systems – *ISACA*

The process of protecting information by preventing, detecting, and responding to attacks – *National Institute of Standards and Technology* (NIST)

What makes Cyber Risk Challenging?

Why is Cyber Risk Challenging?

- What makes cyber risk different from other risks we supervise?
  - Dynamic Nature – Evolving Threats
    - Lack of Geographic Barriers
    - Specialized Knowledge Gap
  - Applicability to Current Practices
  - Absence of Guidance/Standards

difficult to know (who, where, what, how)

- What other risks do we supervise that share these traits?

- How do our supervisory practices promote or deter us from supervising this risk?

FBI: national
CIA: international

Do you Allow Bank Q: hack back transaction? → "country hacking"? → who should be liable?

What makes Cyber Risk Challenging?

Identifying and addressing vulnerabilities is a constant game of cat and mouse for our firms, as fast as patches are implemented new vulnerabilities surface.

identify threat
↓
build security
↓
monitor

Vulnerabilities come in many different forms, both internally and externally sourced. They can be categorized as technological, organizational, human, and even physical.

- Hardware, software, network, or system implementation and hygiene can create technological weaknesses.
- A lack of awareness of threats/vulnerabilities, incomplete asset inventories, inadequate incident response, and weaknesses in/over-reliance on vendors can create organizational vulnerabilities.
- Exploitation of human behavior, such as trust and curiosity, coupled with a lack of effective security awareness training, can make humans a vulnerability to any institution. Even disgruntled employees could pose a vulnerability.
- Theft, tampering, device failure, and introduction of infected media can open the door for attack through physical means.

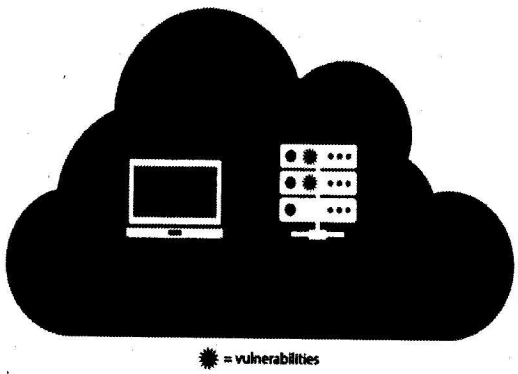


Image: Vulnerabilities are weaknesses resulting from many sources, including technological, organizational, human, and physical. Sources may be internal or external.

What makes Cyber Risk Challenging?

One of the primary challenges with monitoring and responding to cybersecurity risk is the constantly evolving threat landscape.

Some examples of cybersecurity threats include:

- **Distributed denial of service (DDoS):** An attempt to degrade and/or make unavailable any online service of a targeted institution by generating overwhelming traffic or requests from multiple sources.
- **Malware:** Software that is designed to damage and perform unwanted actions into the system. Malware includes viruses, worms, or Trojan horses that are used to delete files or simply gather data without the user's knowledge.
- **Phishing:** An attempt to gain sensitive information like passwords and usernames by using legitimate-looking emails and attempting to gain personal information from those who respond to the emails. These emails can insert malware into a network that can then spread across the institution and steal data from other personnel.
- **Ransomware:** A threat which will restrict access to your computer system data and will ask for a ransom in order for the restriction to be removed. The ransom is generally paid through online payment methods.

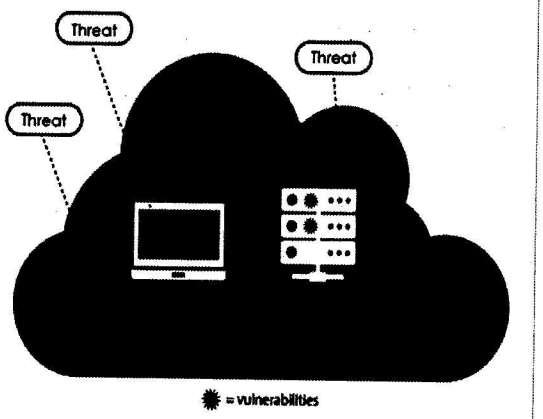


Image: Threats often take advantage of internal and external vulnerabilities.

Threats could include entry from third parties that are aimed at exploiting interconnections of firms and service providers.

What makes Cyber Risk Challenging?

Across the industry it is recognized that cybersecurity cannot be fought alone and, thus, the sharing of cybersecurity threat intelligence and vulnerability compromises is also important to an institution's ability to keep pace with this dynamic threat landscape and prevent costly incidents from occurring.

Incidents may include but are not limited to:

- unauthorized scans or probes,
- denial of service,
- social engineering,
- unauthorized entry,
- malicious code or virus,
- security breach or potential security breach,
- networking system failure (widespread), and
- application or database failure (widespread).

In financial institutions, there are millions of possible signs of incidents that may occur each day. These are often recorded by logging and computer security software. A financial institution needs to be able to filter these logs quickly to identify possible security incidents, and automation is generally necessary to conduct this analysis.

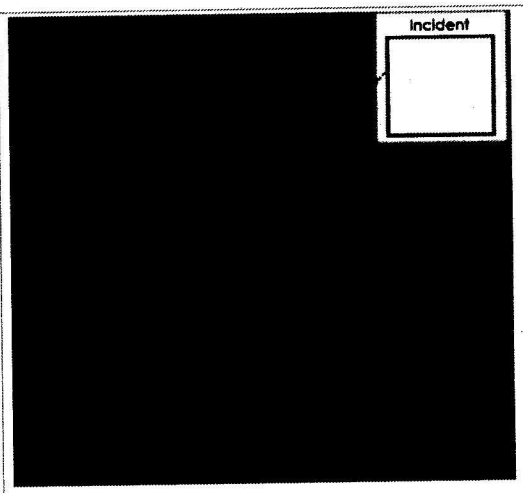
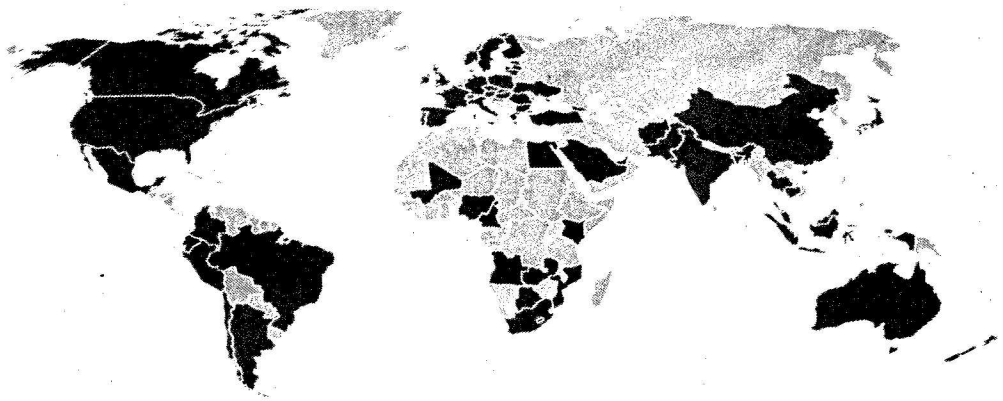


Image: A threat becomes an incident when there are violations of computer security policies, acceptable use policies, or standard computer security practices.

What makes Cyber Risk Challenging?

No locale, industry or organization is bulletproof when it comes to the compromise of data.



2016 Data Breach Investigations Report by Verizon captured incidents affecting organizations in 82 countries and across a myriad of industries.

OPM

What makes Cyber Risk Challenging?

Some of the biggest Security Breaches reported so far in 2016 target personal information that could be used fraudulently in the banking sector.

FACC • $54.5 million	**University of Central Florida** • 63,000 records	**US Dept. of Justice** • 30,000 employee records	**Internal Revenue Service** • 700,000 records
UC Berkeley • 80,000 records	**Snapchat** • 700 records	**21st Century Oncology** • 2.2M patient records	**Premier Healthcare** • 200,000 patient records
Verizon Enterprise Solutions • 1.5M customer records	**Yahoo!** • 500M accounts	**Dropbox** • 68M accounts	**LinkedIn** • 117M accounts
Oracle • Source of data for other POS attacks	**Philippine Commission on Elections** • ~55M voter records	**Wendy's** • Malware on POS	**Newkirk Products** • 3.3M healthcare IDs

Source: https://www.identityforce.com/blog/2016-data-breaches

What makes Cyber Risk Challenging?

The Financial Services industry continues to be a major target.

Finance industry accounted for 8% of private industry incidents reported in 2016.

Industry	Total	Small	Large	Unknown
Accommodation (72)	362	140	79	143
Administrative (56)	44	6	3	35
Agriculture (11)	4	1	0	3
Construction (23)	9	0	4	5
Educational (61)	254	16	29	209
Entertainment (71)	2,707	18	1	2,688
Finance (52)	1,368	29	131	1,208
Healthcare (62)	166	21	25	120
Information (51)	1,028	18	38	972
Management (55)	1	0	1	0
Manufacturing (31-33)	171	7	61	103
Mining (21)	11	1	7	3
Other Services (81)	17	5	3	9
Professional (54)	916	24	9	883
Public (92)	47,237	6	46,973	258
Real Estate (53)	11	3	4	4
Retail (44-45)	370	109	23	238
Trade (42)	15	3	7	5
Transportation (48-49)	31	1	6	24
Utilities (22)	24	0	3	21
Unknown	9,453	113	1	9,339
Total	64,199	521	47,408	16,270

Finance industry accounted for 35% of all reported incidents with a confirmed data loss.

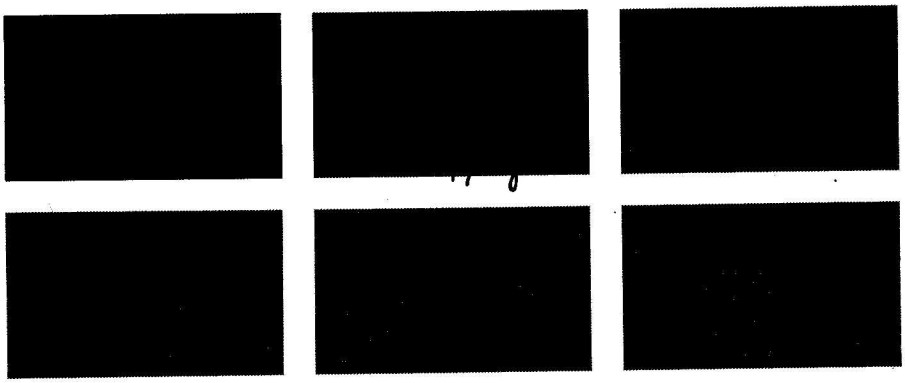
Industry	Total	Small	Large	Unknown
Accommodation (72)	282	136	10	136
Administrative (56)	18	6	2	10
Agriculture (11)	1	0	0	1
Construction (23)	4	0	1	3
Educational (61)	29	3	8	18
Entertainment (71)	38	18	1	19
Finance (52)	795	14	94	687
Healthcare (62)	115	18	20	77
Information (51)	194	12	12	170
Management (55)	0	0	0	0
Manufacturing (31-33)	37	5	11	21
Mining (21)	7	0	6	1
Other Services (81)	11	5	2	4
Professional (54)	53	10	4	39
Public (92)	193	4	122	67
Real Estate (53)	5	3	0	2
Retail (44-45)	182	101	14	67
Trade (42)	4	2	2	0
Transportation (48-49)	15	1	3	11
Utilities (22)	7	0	0	7
Unknown	270	109	0	161
Total	2,260	447	312	1501

Source: http://www.verizonenterprise.com/verizon-insights-lab/dbir/2016/

What makes Cyber Risk Challenging?

Motivations for generating new threats are varied, but a majority are financially driven.

Motivations could include....



Secondary Motive:
Aid in or distract from a different attack

What makes Cyber Risk Challenging?

Attackers motives also continuously evolve, making it a challenge to anticipate threats before they occur.

Threats evolve with attackers motives...

Blackmail Executives	Disrupt Infrastructure	Accelerate Espionage	Expose World Leaders
Attacker breached executive email to **blackmail** against the release of *The Interview,* and published **humiliating** emails after the movie's release.	Attacker infiltrated Ukraine's power grid using multiple attack methods in order to **stop electricity delivery to citizens** as retribution during a political conflict.	Attacker stole federal background checks to construct a **massive database of individuals** with access to sensitive government information for espionage purposes.	Attacker breached documents and emails of a law firm and used them to expose **personal financial dealings** of world leaders and high-net-worth investors to pressure financial reform.
Sony Pictures Breach	**Ukraine Breach**	**OPM Breach**	**Mossack Fonseca Breach**

How have FIs responded to Cyber?

How Are Financial Institution's Responding to Cyber?

What trends are you seeing in terms of response?

Have trends been more cultural, financial, organizational, or practical ?

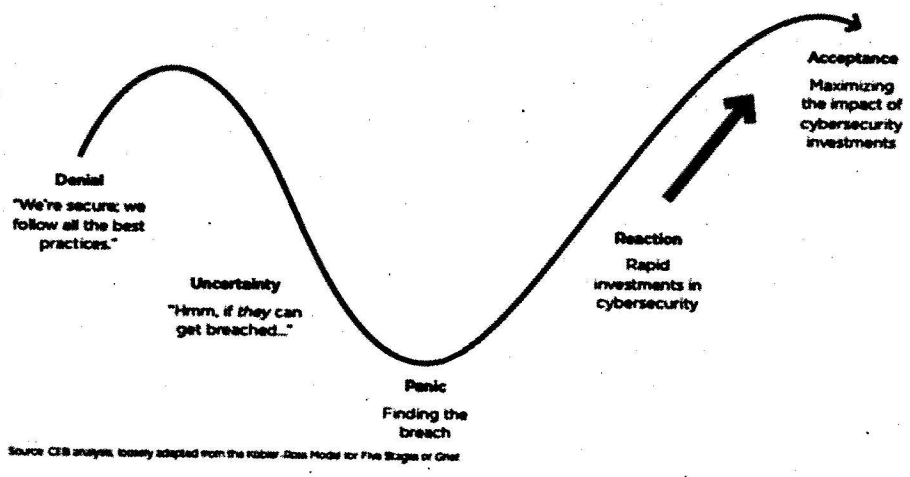
Where is improvement noted?

Where is improvement needed?

How have FIs responded to Cyber?

Culturally

Most financial institutions have accepted that cybersecurity risk can be managed, but never eliminated.



Source: CEB analysis, loosely adapted from the Kübler-Ross Model for Five Stages of Grief

Board discussions, top risk reports, strategic plans, and budgets are now showing recognition of the significant threat cybersecurity is to the financial services industry.

How have FIs responded to Cyber?

Financially

Financial institutions of all sizes and complexities are spending more on information security and all indications show that this trend will continue.

CYBERCRIME WILL COST BUSINESSES OVER $2 TRILLION BY 2019

Hacktivism Professionalising and Going After Bigger Targets

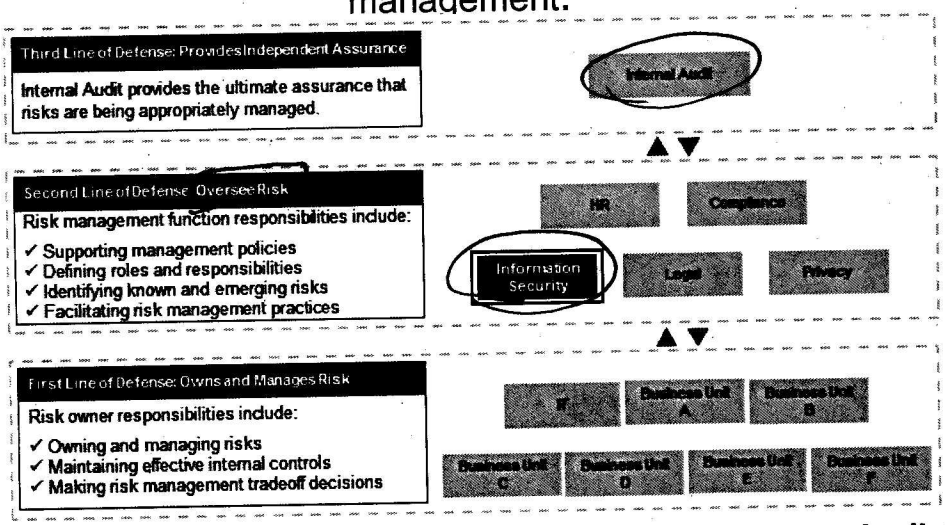
Hampshire, UK - 12th May 2015: New research from leading market analysts, Juniper Research, suggests that the rapid digitisation of consumers' lives and enterprise records will increase the cost of data breaches to $2.1 trillion globally by 2019, increasing to almost four times the estimated cost of breaches in 2015.

The research, entitled 'The Future of Cybercrime & Security: Financial and Corporate Threats & Mitigation', has found that the majority of these breaches will come from existing IT and network infrastructure. While new threats targeting mobile devices and the IoT (Internet of Things) are being reported at an increasing rate, the number of infected devices is minimal in comparison to more traditional computing devices.

How have FIs responded to Cyber?

Organizationally

Some firms are changing their organizational structures, especially within risk and operations, to provide stature and support to cybersecurity risk management.



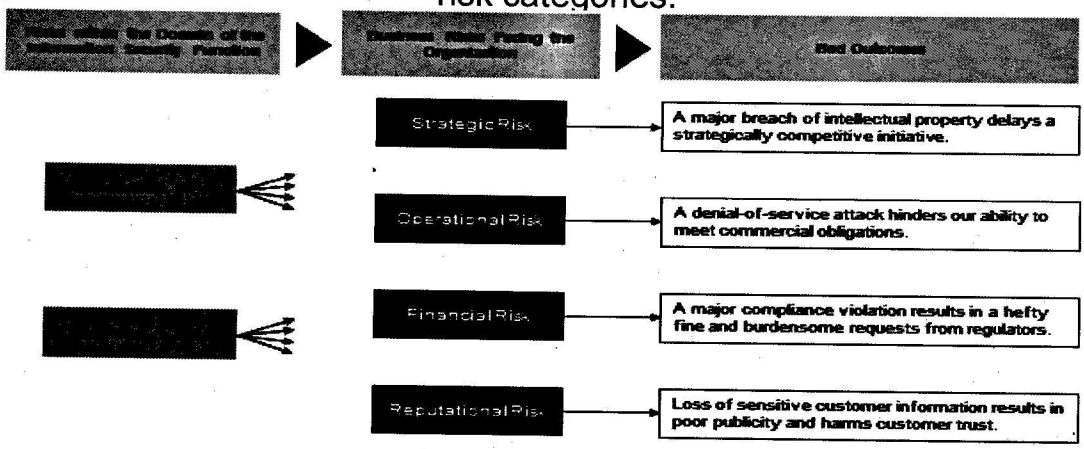
oversee

IT (operations) and Information Security (risk) are more commonly divided.

How have FIs responded to Cyber?

Practically…

Cybersecurity risks are being considered not only from an information security or IT Risk perspective, but also through the lens of other major risk categories.



Uncontrolled cybersecurity risk can hinder a firm's ability to achieve its strategic objectives.

How have FIs responded to Cyber?

While change has been observed, the industry has room for improvement

KPMG's 2016 Banking Outlook Survey found that 12% of the 100 Bank Executives Surveyed still do not have insight into whether their information security has been compromised by cyber attacks over the last two years.

Results from executives one or two tiers below the C-suite were even more disconnected from their institution's cybersecurity history.

The full report: ***"The Need For Speed,"*** can be accessed at: http://www.kpmg.com/us/2016bankingindustryoutlooksurvey.

FSR 2015 cyber security:

What Supervisory Tools Apply?

What Supervisory Tools Apply?

What tools exists that can be applied to cybersecurity supervision?

What has hindered development of more supervisory guidance in this space?

How do you currently push your institution's to employ greater cybersecurity risk management practices?

Does the nature and pervasiveness of cybersecurity risk push the industry to react without formal guidance?

What and who should drive supervisory guidance for cybersecurity?

capital ; examine : on-site

hardly ; proposal → public feedback = not willing ⇓ dynamic change guidance not trust...

What Supervisory Tools Apply?

Today's Domestic Tools with Broad Applicability:

URSIT	FFIEC IT Handbooks	Gramm-Leach-Bliley Act (GLBA)	Sound Practices
• Interagency rating system used to assess financial institutions on IT audit, management, development and acquisition, and support and delivery. • Focused on data security and other risk management factors ensuring quality, integrity, and resiliency of IT	• Guidance for financial sector on IT risk, including business continuity , retail payments, and information security, which have been updated to incorporate cybersecurity expectations	• Act required each agency to establish controls for safeguarding of financial institution's customer information. • Interagency Guidelines established in 2000 outline administrative, technical, and physical control program expectations.	• Intended to minimize immediate systemic effects of wide scale disruption by wide-scale disruption to critical financial markets by setting expectations for recovery capacity

What Supervisory Tools Apply?

Today's Domestic Tools with Cyber Focus:

NIST Cybersecurity Framework

- Industry agnostic, voluntary framework to understand, manage, and reduce cybersecurity risk.
- Intended to provide a broad framework that can be customized for business sectors and organizations from any industry
- This framework also encourages better communication and awareness between business leaders and IT functions.

FFIEC Cybersecurity Assessment Tool

- Interagency, voluntary self-assessment tool that is applicable to all size institutions
- Intended to help assess cyber risk and determine preparedness of an organization
- Provides repeatable and measurable processes to determine if appropriate controls and risk management practices have been implemented relative to the firm's risk profile.
- The CAT incorporates key concepts from NIST's Cybersecurity Framework

5 core function
① identify ② predict ③ detect ④ respond ⑤ recovery

What Supervisory Tools Apply?

International Guidance:

Committee on Payments and Market Infrastructures (CPMI) and International Organization of Securities Commissions (IOSCO)

Guidance on Cyber Resilience for Financial Market Infrastructures

- First internationally agreed guidance on cyber security for financial industry.
- Intended to add momentum and instill international consistency to industry's ongoing efforts to enhance FMI's ability to pre-empt cyber attacks, respond rapidly and effectively to them, and achieve faster and safer target recovery objectives
- The purpose was "not intended to impose additional standards on FMIs beyond those in the Principles for Financial Market Infrastructures, but provide greater detail on preparation and measures that should be taken to enhance cyber resilience to minimize the escalating threats on financial stability.

How can we supervise Cyber?

banks like sitting duck.
~~bank like electronic~~ => punishment: less.

How can we supervise Cybersecurity?

- What makes you most uncomfortable about cybersecurity supervision?
- What challenges do you see in applying traditional supervisory practices?
- What risk areas do you see this impacting?
- How do you think resource and training issues can be tackled?

How can we supervise Cyber?

Broad Supervisory Considerations

Cybersecurity should be part of an institution's ongoing ability to: (important)

identify and manage salient risks;
maintain operations and services;
protect its customer information, safety and soundness, and reputation;
maintain public confidence;
limit, where applicable, contagion risks to the rest of the industry

These abilities should be an input into risk assessments, supervisory plans, examination procedures, and ongoing supervision programs.

How can we supervise Cyber?

Cybersecurity/IT Focused Supervision

Portfolios	Approach
Smaller, less-complex financial institutions	• Incorporate cybersecurity risk management practices, controls, and response protocols into elements of IT examination work. • Emphasize use of risk management programs like business continuity, vendor risk management, and information security programs – including incident response, training, and issue escalation.
Larger, more-complex financial institutions	• Consider targeted work against specific topics or risk factors • Incorporate into other IT and broader Risk Management examinations • Emphasize impact on risk management programs like business continuity, incident response, vendor risk management, and information security programs and incorporate into reviews of such programs. • Remain cognizant of how cybersecurity could impact other banking programs like Enterprise Risk Management, new product/service deployment programs, operational and compliance risk focused examinations, and even Corporate Governance.

How can we supervise Cyber?

Cybersecurity in scope of integrated supervision

Cybersecurity perspectives vary, but are important across portfolios and supervisory perspectives.

Safety & Soundness Perspective

- Understand how cybersecurity risks are incorporated into the broader corporate risk management practices
- Evaluate the level of understanding and involvement of the board of directors (board) and senior management in oversight of this risk
- Observe the institution's culture to determine if it reflects awareness and consideration for the potentially widespread impact of this risk

Consumer Compliance Perspective

- Ensure that the institution's identity theft prevention program, credit bureau reporting, and card issuance practices are comparable and scalable to the potential threat of a cybersecurity incident
- Evaluate a financial institution's compliance function roles and responsibilities pre- and post-incident
- Understand how cybersecurity risks are considered in the institution's compliance risk management program

How can we supervise Cyber?

Cybersecurity transcends many other supervisory topics

Capital Planning

- Determine if the risk profile necessitates consideration of cyber events as Idiosyncratic risk or stress scenarios

Compliance

- Recognize the extensive legal and reputational impacts of a cyber events
- Understand implications of consumer compliance laws for reissuance of and restitution for credit cards, identity theft monitoring, and customer notification protocols
- Consider how vendor risk management especially where customer information resides with a 3rd party are managed.

Liquidity Management

- Recognize cybersecurity events have the potential to paralyze clearing and settlement systems, delete or corrupt client data, or simply make websites unavailable.
- Determine if contingency funding plans account for events of sizable scope and duration

Enterprise Risk Management

- Review risk identification and aggregation practices to see how they account for potential interplay between cyber and other risk stripes
- Understand escalation protocols and reporting lines for cyber events and ongoing risk management

Audit

- Evaluate and understand how audit incorporates new and emerging risks and technologies.

How can we supervise Cyber?

Ongoing Supervision Considerations

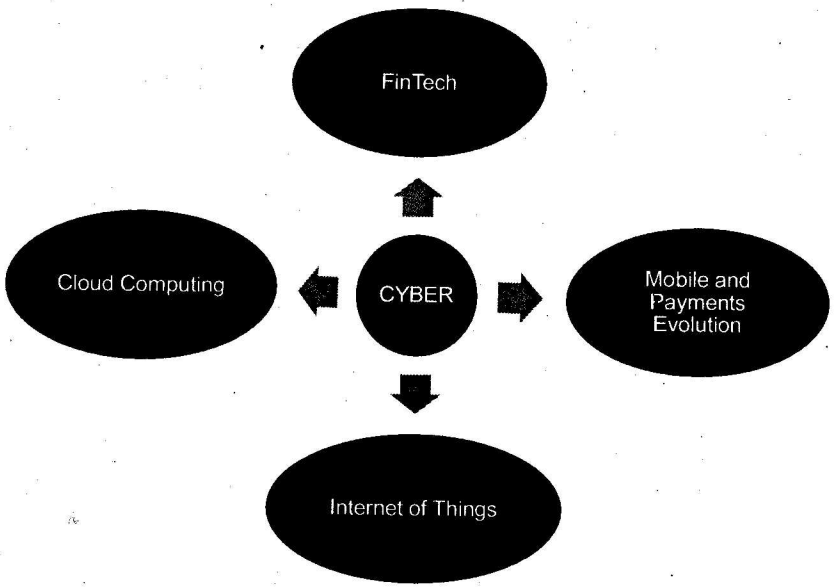
- **ERM reporting**: Risk reports to the board and senior management highlighting top risks may provide insight into the institution's awareness, level of concern, and approach/actions to mitigate cybersecurity risk.
- **Board discussions**: Information conveyed to the board often influences budget and strategic decisions. The inclusion of cybersecurity in such discussions can be an informative perspective into the institution's preparedness and ultimate response.
- **Scenario selection**: Scenarios are a widely used risk management tool across a variety of risk categories and can be a good indication of management's mindset if they include cybersecurity. Regardless of an institution's size or complexity, some forms of scenarios are likely used. Scenarios that might consider cybersecurity could be related to business resumption/disaster recovery, liquidity risk management, capital planning, or even in living wills or recovery/resolution planning.
- **Audit reports**: Whether a broad-based IT audit report from a community bank or a cybersecurity strategy audit from an larger audit department, such reports can provide valuable information on an institution's preparedness for and resilience to cyber attacks that could influence changes to the institution's risk profile.
- **Press releases**: Often these could be our first indication that there is an incident that directly or indirectly affects an institution. Publically available information could also provide details to help guide conversations with supervised institutions.

While in no way an exhaustive list, the connections or impact points that cybersecurity risk has across many facets of a financial institution are vast and there are many information sources to consider in the development of an institution's overall risk profile.

How can we supervise Cyber?

Impact of Emerging Technologies and Ventures

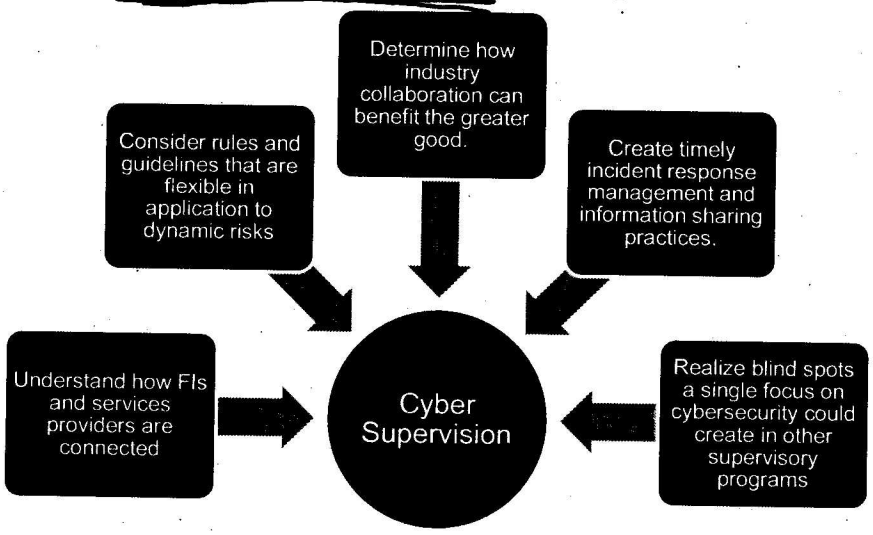
Our supervisory roles will continue to be challenged as cybersecurity risk has a correlation to many of today's financial sector trends.



How can we supervise a moving target?

Supervision of Cybersecurity

Unconventional and unique supervisory practices may need to be considered in order to effectively ensure the safe and soundness of the financial services sector in today's world.

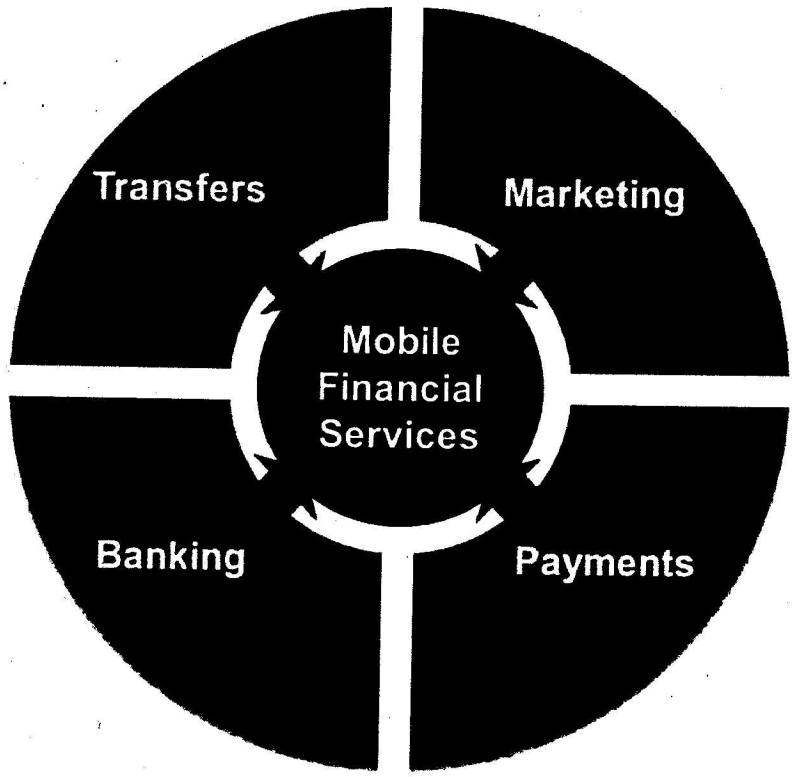


IT Risk: Mobile Banking and Payments

Agenda – Purpose of Presentation

- Define Mobile Financial Products
- Describe Mobile Banking functionality, drivers and risks
- Describe Mobile Payments functionality, drivers and risks
- Identify the key supervisory practices for understanding and evaluating mobile financial products

Mobile Financial Products



Current and Emerging Payment Models

Business models under development

1. Network operator centric (e.g. Verizon)
2. Bank centric
3. Managed by a trusted third party (Google, Paypal, Square, etc.)

"Major players" category is getting crowded

- Mobile network operators
- Handset / SIM chip manufacturers
- Banks
- Card associations
- Payment networks
- Prepaid companies
- Merchants
- Internet search and payment services providers
- Proprietary payment application providers

Business Drivers

Value add

- Potential for scale in fragmented markets
- Ability to focus on new markets (unbanked, under-banked)
- Innovation that bypasses current infrastructure limitations
- Major influence on efficiency and access to payment services

Business Challenges and Risks [USA]

Challenges/Risks

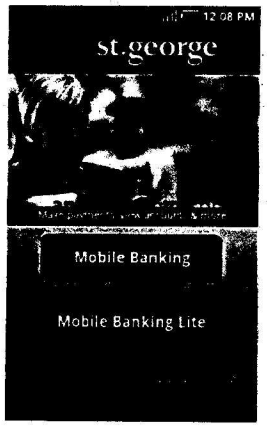
- Unclear regulatory oversight in emerging markets
- Potential unintended consequences – risk, fraud, security
- Data governance and vendor management
- Unclear impact on consumers when innovations or innovators fail
- Unclear responsibility for regulatory oversight / consumer protection
- May create a major single point of failure potential

Mobile Banking

Mobile Banking (insured depository institutions)

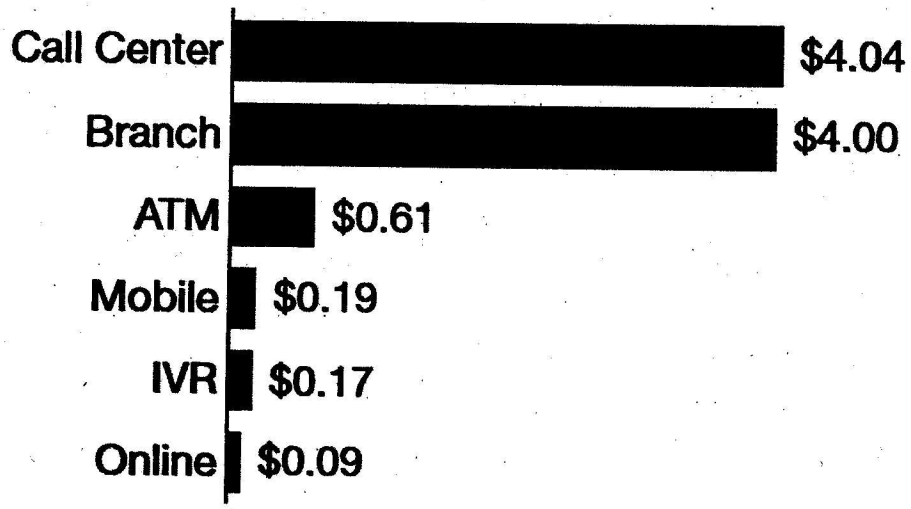
Use of a mobile device
- cell/smart phone or
- tablet computer

Conduct banking activities such as
- balance inquiry
- account alerts
- bill payment



Transaction Costs by Banking Channel

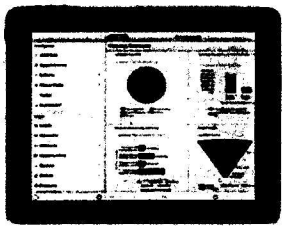
Average transaction cost in the US
(includes labor and IT costs)



Source: CEB TowerGroup

Mobile Application Types

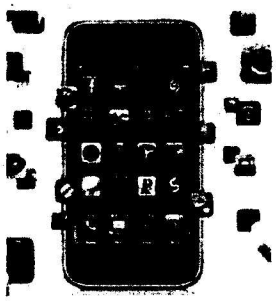
Native Client



Application and Application data reside on device.

Using the language and platform of the mobile device.

Hybrid Client

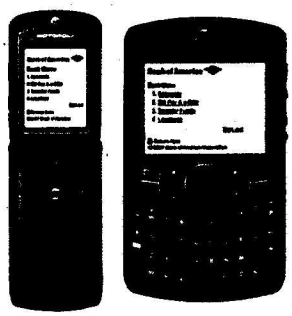


Application Resident on device; data sourced from "online" sources.

Browser embedded within the app, based on HTML5.

e.g., Netflix, Linkedin, Facebook, Yelp, etc.

Web Client

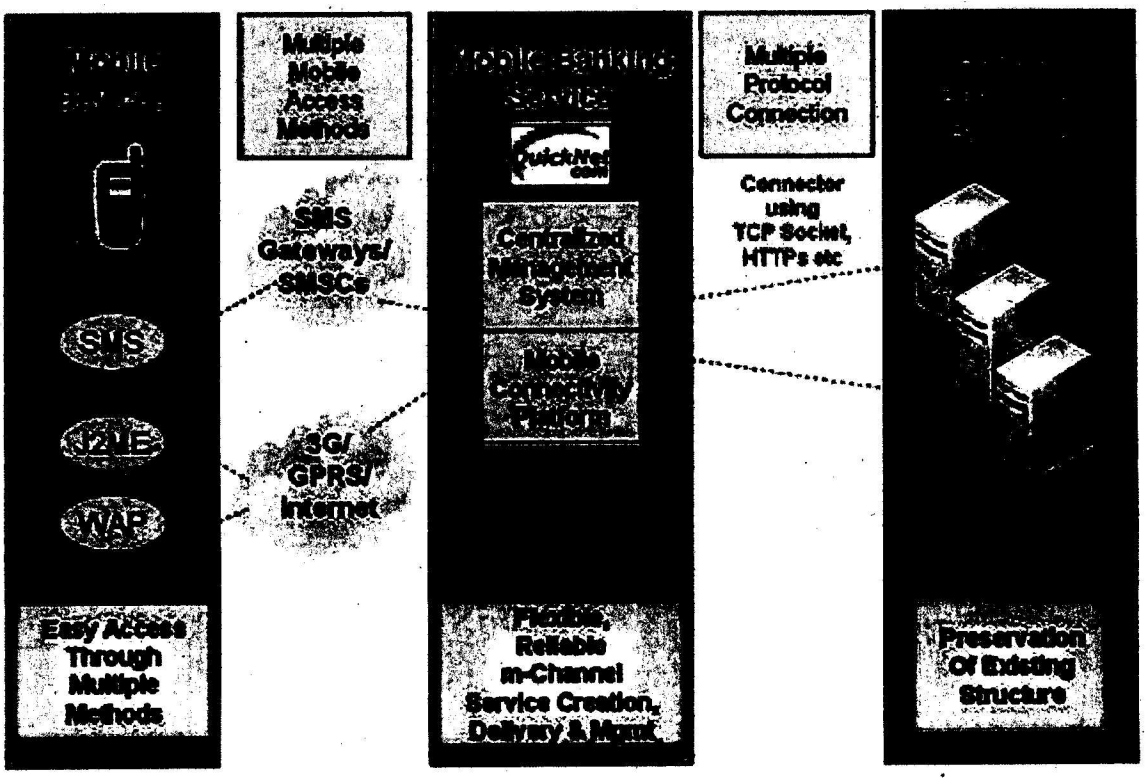


Neither application nor data reside on device.

Browser or small downloadable client.

Supports also older phones.

Integration with Existing Infrastructure

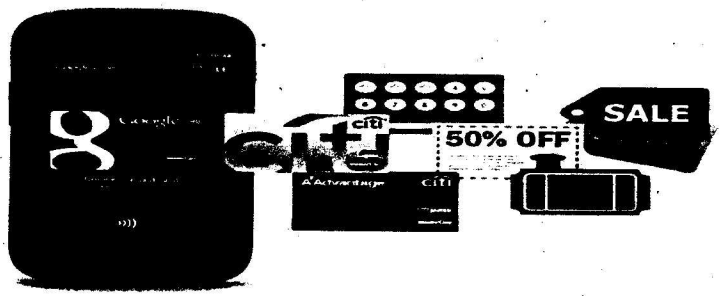


Mobile Payments

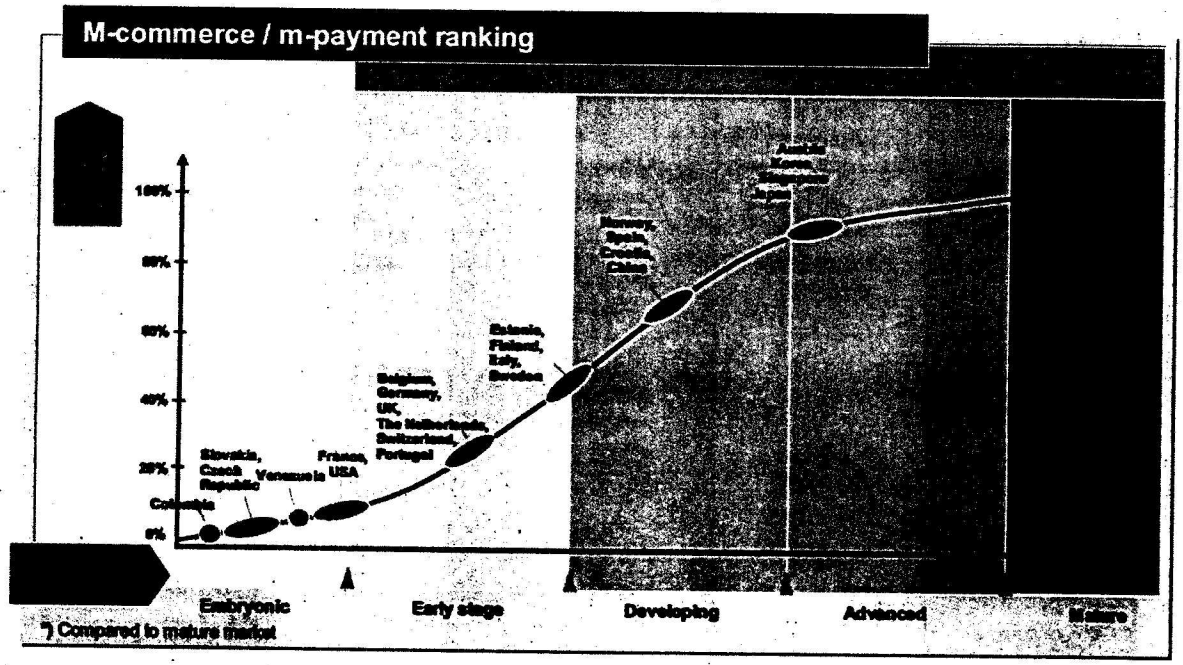
Mobile Payments (many types of companies)

Mobile banking and payments are not interchangeable

- uses the same mobile devices to initiate payments
- from a person to person(s) or businesses

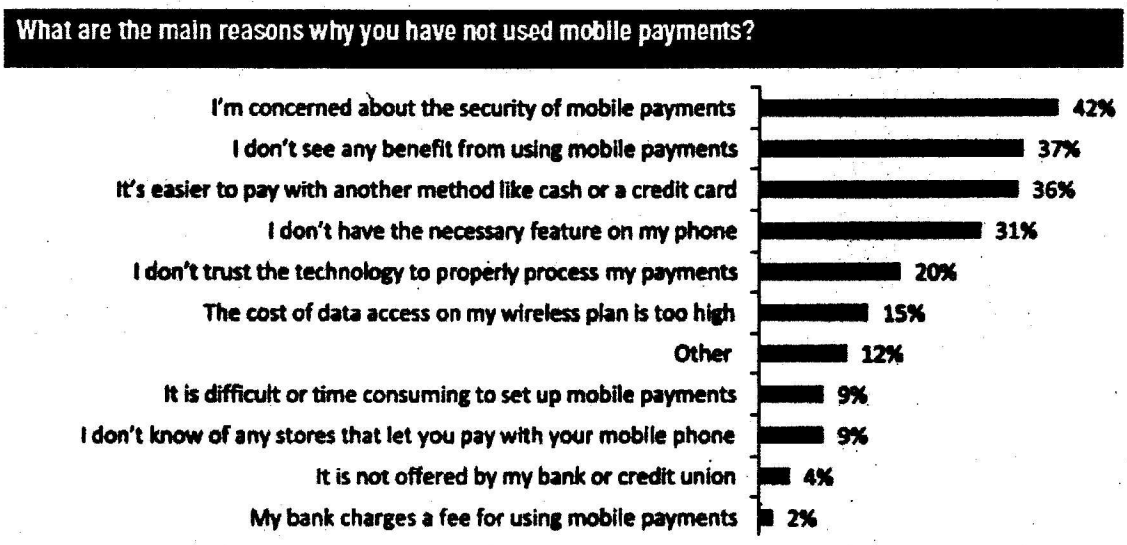


Global Mobile Commerce Rankings



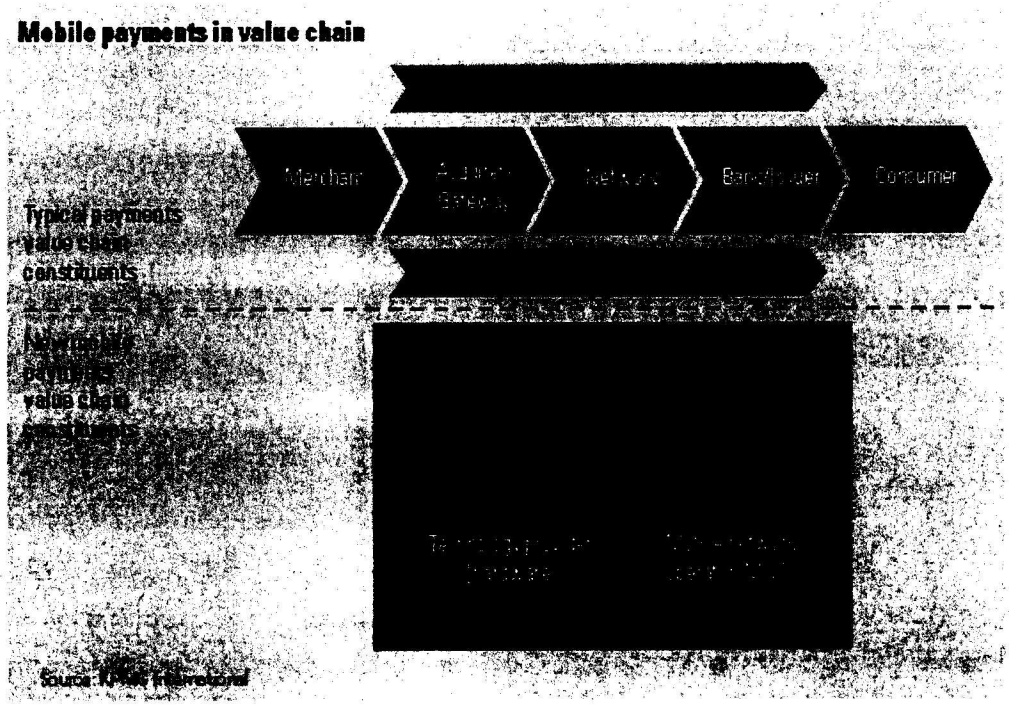
Source: Arthur D. Little M-Payment Report

Customer's Perception



Source: Consumers and Mobile Financial Services Study (Board of Governors of the Federal Reserve System – March 2012)

Mobile Payments in Value Chain



Mobile Payments

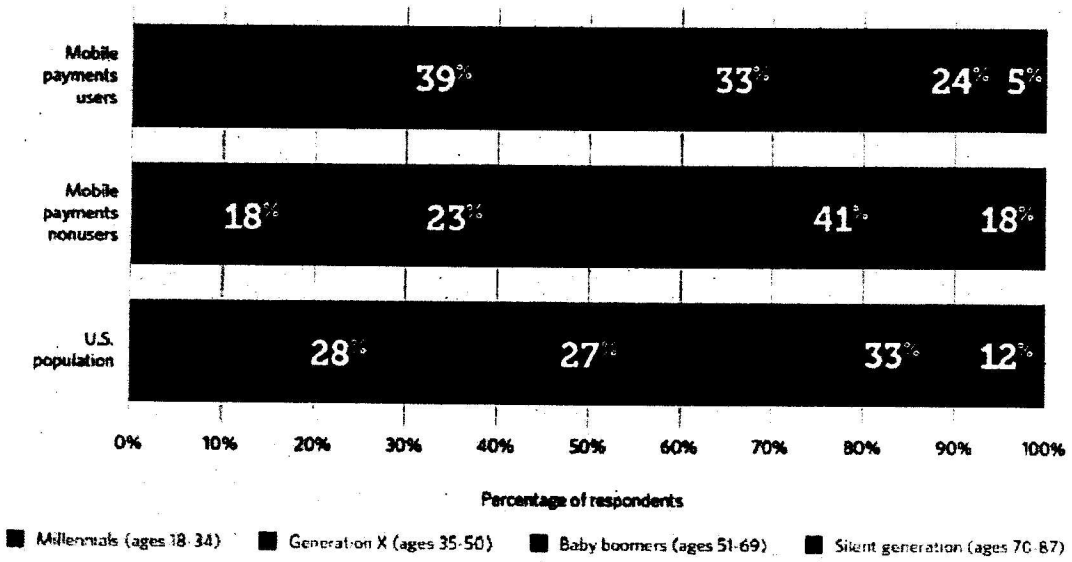
Mobile payment technologies			
NFC companion devices			
Embedded NFC	Uses a	Uses existing contactless card standards, enables access to multiple accounts via mobile wallet interface, provides some additional security within SE on the handset.	
SMS text	Remote payments, primarily for digital content.	Ubiquitous capability available on the vast majority of handsets.	
Voice	A niche technology that provides mostly account servicing and bill payments, some mobile payment authorization conducted via voice.	Person to person interaction, opportunities for dynamic cross-selling.	High cost in two agent situations and inefficient data communications.

Source: KPMG International 2011

The Mobile Payments Generation Gap

72% of Mobile Payments Users Are Millennials or Generation Xers

Mobile payments user status by generation, compared with the total population



Establishing Mobile Security Policies

- Define the policies from a threat and controls perspective:
  - Utilize existing policies and standards for guidance
  - Align to corporate policies, industry standards, and applicable regulations
- Consider the policy impact on business functions and user experience
- Align policies with capabilities of management solutions
  - Identify what policies can be enforced, and how policies are managed and pushed
  - Consider how enforced policies will be tested and validated
  - Consider the impact of policies on security administration and supporting infrastructure
- Adopt multiple policies for differentiated use cases as needed; limit where possible.

Key Mobile Policy Elements

- Data Storage
- Data Sharing
- Device Connectivity
- Device Authentication
- Data and Device Wipe Mechanisms
- Feature Controls
- Applications Allowed

Do you allow customer connect WiFi? unsecure WiFi?

Supervisory Considerations

- Controls over mobile product development including interoperability of complex mobile payment systems
- Controls over 3rd parties including non-bank partners, networks, vendors, and service providers including RFP approach and SLAs
- Coverage over legal and compliance risks
- Implementation of customer exposure limits including fraud detection and response plan
- Implementation of Security and customer education requirements
- Transaction authentication and authorization practices

who own the data?
who own the phone?
who should be liable to the disclosure?

HTTPS: is unsecure.

IT Risk: FinTech

Agenda – Purpose of Presentation

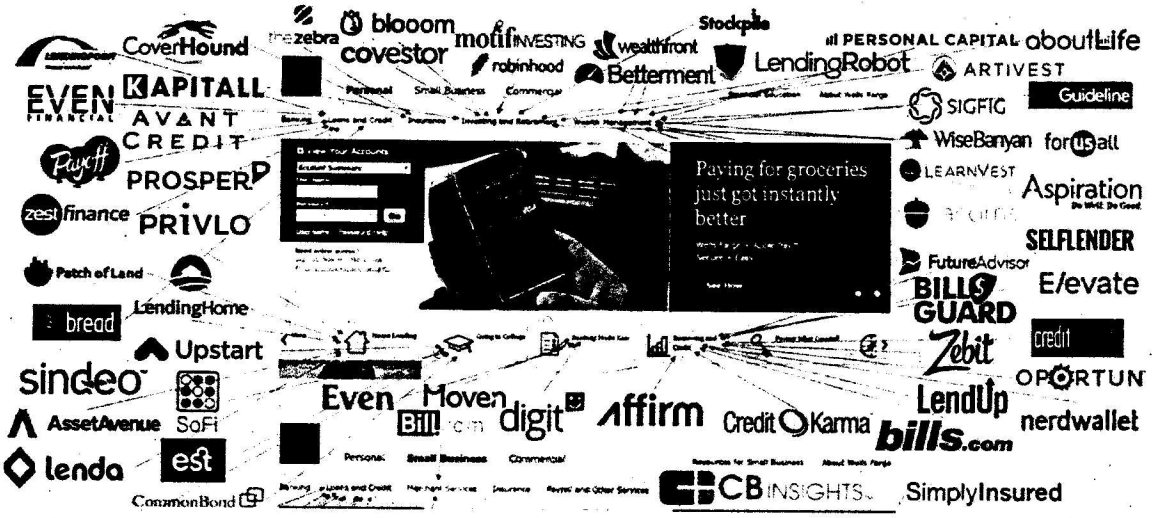
- Define fintech
- Describe the importance of fintech to supervisory community
- Summarize Federal Reserve's and other U.S. regulators' response to fintech innovation and growth
- Describe various fintech segments
- Explain important developments and concepts in alternative lending

What Is Fintech?

ATM. → Online Banking

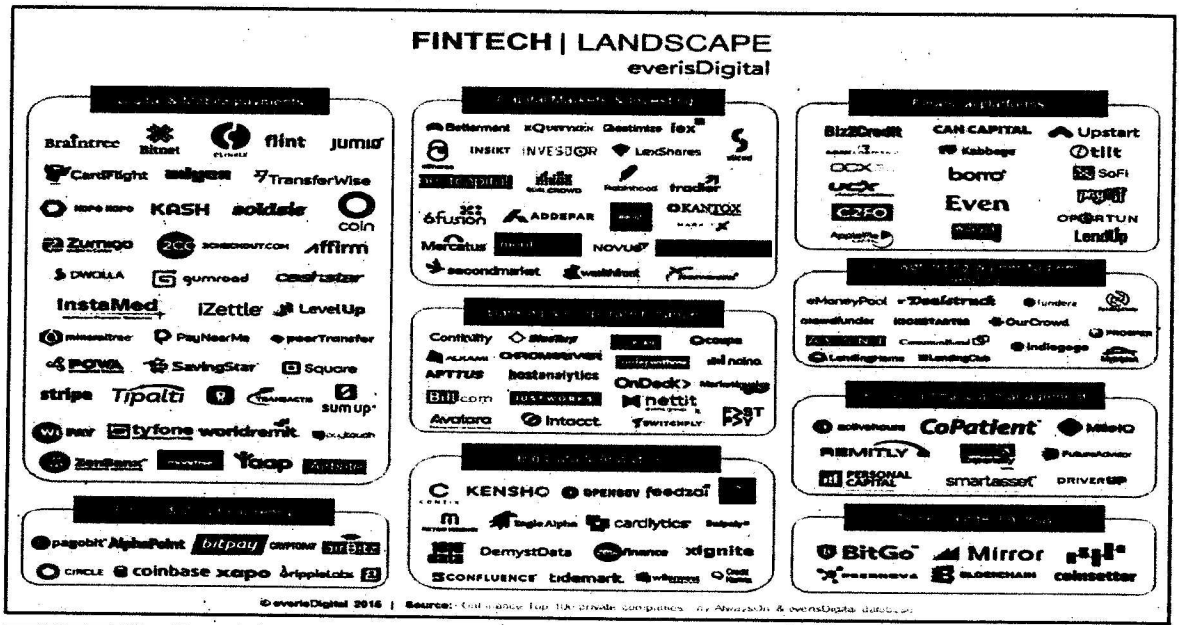
- Fintech is an industry composed of companies that use technology to make financial systems and the delivery of financial services more efficient

Unbundling of a Bank



Source: CBInsights; https://www.cbinsights.com/blog/disrupting-banking-fintech-startups/

Fintech Innovations are Transforming Financial Services for Consumers and Businesses



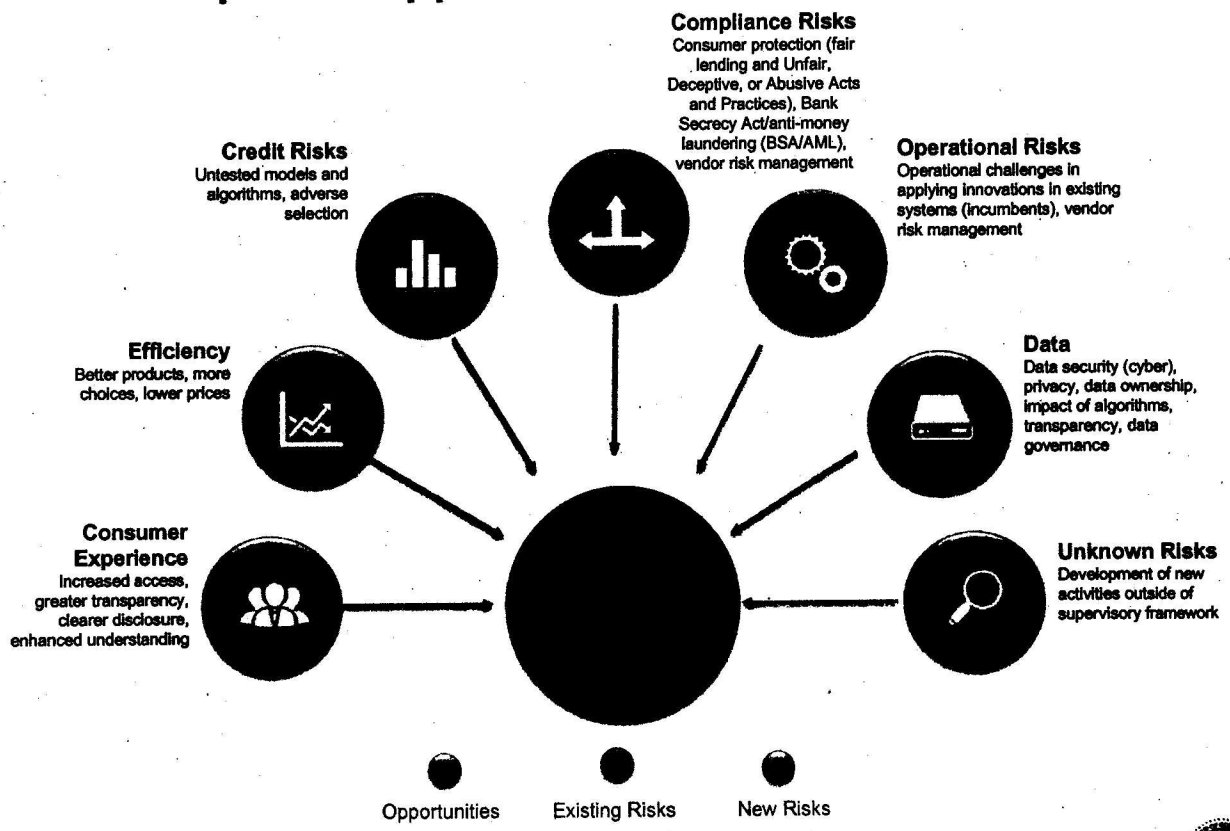
According to one report, global investment in fintech companies totaled $19.1 billion in 2015 ($13.8 billion in the United States).

One firm (Venture Scanner) is tracking 1,379 fintech companies.

Why Do Regulators Care?

- Fintech and banks are connecting in multiple ways:
  - Banks invest in fintech companies
  - Banks establish start-up programs to incubate fintech companies
  - Banks partner with fintech companies:
    - Originate loans for fintech lenders
    - Retail business platform provider – cobranding arrangements
    - White label/private label arrangements
    - Referral arrangements for a fee
  - Banks acquire fintech companies
  - Banks launch own fintech solutions

Fintech Impacts: Opportunities & Risks



Source: This figure was inspired and derived from a similar figure in the report *Technological Innovation and the Dutch Financial Sector* published by *De Nederlandsche Bank*

Initial Regulatory Response to Fintech Innovation

- **Federal Reserve System (FRS):**
  - Governor Lael Brainard Steering Committee – Overarching umbrella for all Federal Reserve System efforts
  - Fintech High-Priority Initiative – Multidisciplinary working group
  - Other efforts relating to payment systems and the Basel Committee
  - BSA/AML and distributed ledger workstreams

- **Office of the Comptroller of the Currency (OCC):**
  - *Responsible Innovation* whitepaper (March) and related public forum (June)
  - Considering limited-purpose fintech charter and regulatory sandbox

- **Federal Deposit Insurance Corporation (FDIC):**
  - *Supervisory Insights* article on marketplace lending
  - Limited examinations of fintech firms partnering with banks
  - Proposed new third-party lending guidance

- **U.S. Treasury:**
  - Completed request for information (RFI), *Public Input on Expanding Access to Credit through Online Marketplace Lending,* in 2015
  - Issued *Marketplace Lending* whitepaper (after RFI) in May 2016

- **Consumer Financial Protection Bureau (CFPB):**
  - Consumer bulletin on marketplace lenders in March 2016
  - Accepting consumer complaints against marketplace lenders
  - Project catalyst

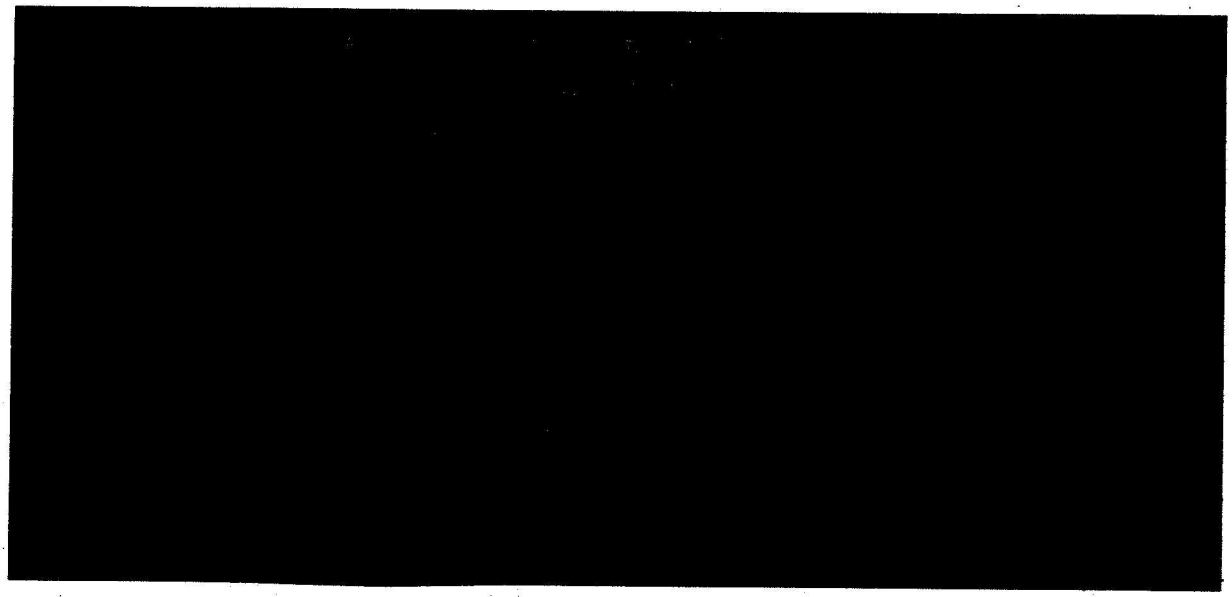
USA's consumer protection √ lower than EU. ∓ compensate customer

1

X

- **Federal Trade Commission:**
  - Hosting a series of forums on marketplace lending beginning June 2016

Sandbox: won't do in USA. ⇒ no waive of the authority.



Lael Brainard
Federal Reserve Governor
April 14, 2016

Federal Reserve's Primary Areas of Fintech Focus

- The Board of Governors of the Federal Reserve System established a multidisciplinary working group that is engaged in a 360-degree analysis of fintech innovation

- Focused on the following fintech segments:

Alternative lending	Savings, investments, financial planning	Digital payments	Blockchain and virtual currency

Data and Technology Ecosystem
Application Programing Interface (API) standards, big data/data analytics, and mobile delivery channel

- Fintech creating **nontraditional platforms** for banking products and services
- Disruption most likely to impact **how financial services are delivered**
- Each fintech area developing at different pace; **not all will be equally disruptive**

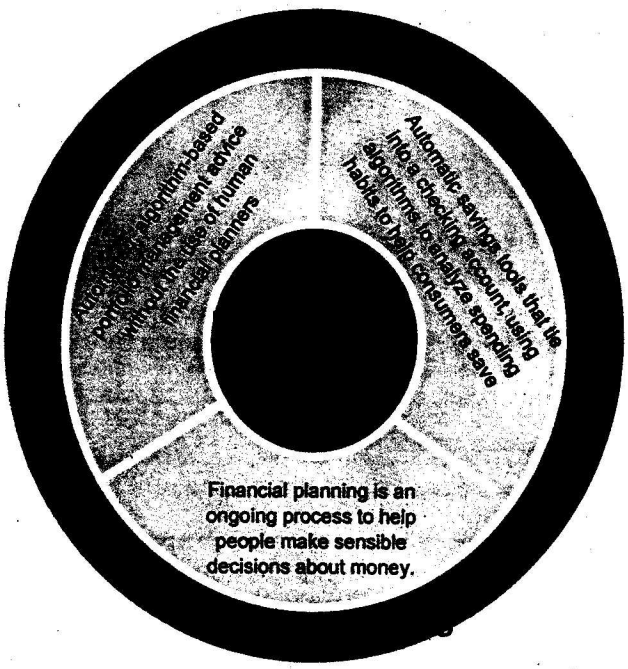
Data application ?

Federal Reserve Fintech Initiative

Work Stream
Market Efficiency and Alternative Lending
Data Aggregation
Savings, Investment and Financial Planning
Payments / Digital Wallets
Blockchain
SMB Survey

Work Stream
Outreach / Public Statements
Convening Power
Bank Service Company Act Options
Chartering / Licensing Position
Innovation Hub / Sandbox Position
Vendor Risk Management Guidance and Supervisory Practices
Fair Lending / UDAP Guidance and Supervisory Practices
BSA / AML Guidance and Supervisory Practices

Savings, Investments, and Financial Planning Segment



Robo-Advisors

wealthfront

Betterment

SIGFIG

Automated Savings Platforms

digit

dyme
pay yourself

SIMPLE

Financial Planning

piggymojo

Even

mint

Source: Federal Reserve System

Payments Segment

Digital wallets are the electronic devices that allow individuals to make e-commerce transactions.

Consumer to

[redacted]

xoom
A PayPal Service

venmo

popmoney

Google wallet

Payments between consumers

Pay

SAMSUNG pay

pay

Consumer to

[redacted]

Consumers pay merchants with credit cards through mobile devices.

[redacted]

Business to Business

DWOLLA

YAPSTONE

[redacted]

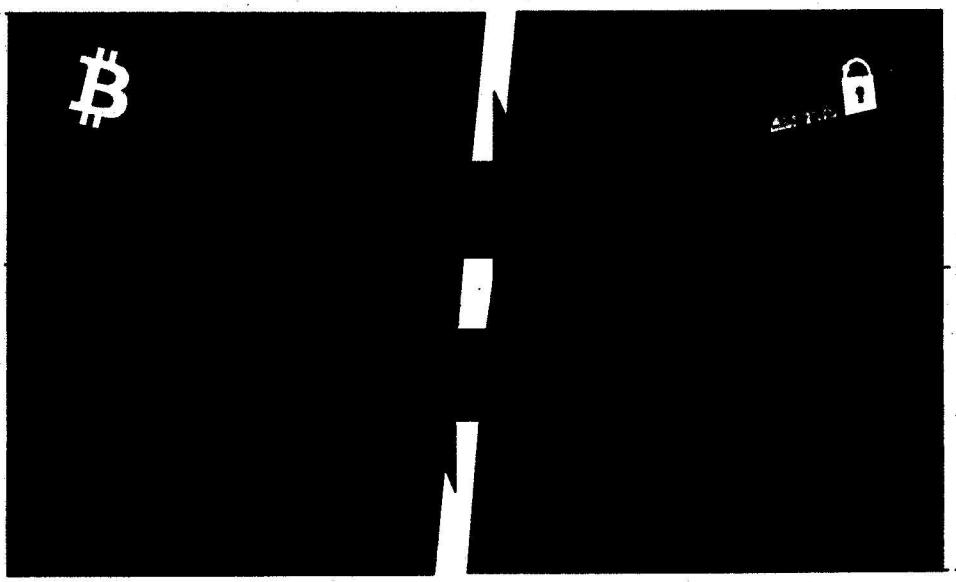
Making Automated Clearing House easier to use

Source: Federal Reserve System

Blockchain Segment

The entire Bitcoin network relies on a Blockchain network

Blockchain could be used to facilitate the exchange of financial assets with less ~~middlemen~~.



Several Blockchain companies are on the rise, e.g.,

- Chain
- Mirror
- ripple

Bitcoin and Blockchain could have vast impacts on the fintech industry.

Source: Federal Reserve System

Data and Technology Ecosystem Segment

The Technology Behind Fintech

Mobile

- Apps, complete with modified user experiences, are being rolled out for consumers' on-the-go financial services needs.

Big Data

- Vast amounts of consumer data
- How to interpret and use it

API

- Programming code allows two software programs to communicate with each other
- Bank transactional data about consumers

Source: Federal Reserve System

Alternative Online Lending Segment

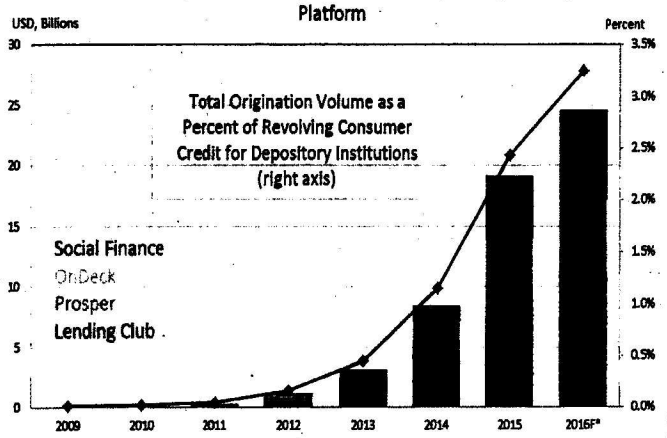
- Alternative Lenders (ALs) are nonbank lenders that focus on the Internet and emerging data-analytic technologies.
  - Technology is used to improve customer experience, lending decisions, customer sourcing, and funding.
- ALs were originally viewed as a competitive threat to banks despite relying on them for loan origination.
- More recently, many banks have established a variety of business engagements with ALs.
  - The System is contacting state member banks to determine the types of ALs and fintech companies with which they are engaged.

AL Landscape

- Most loans are consumer or small business loans.
  - Consumer: Typically 3–5 years, <$35,000, unsecured
  - Small business: Typically <$500,000, <5 years, secured/unsecured
- Growth in loans has been rapid, from virtually nothing pre-crisis, but market shares are still very small.
  - Consumer loans are only about 3 percent of the U.S. market.

Alternative Lending Originations

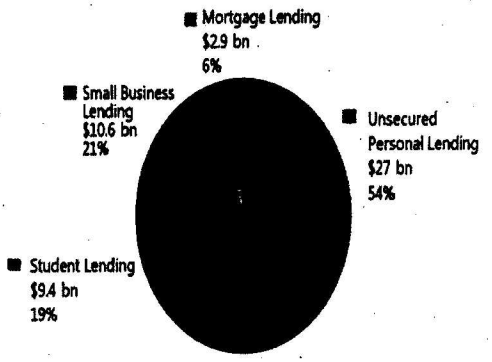
U.S. Marketplace Loan Origination Volume by Year by Leading Platform



*2016 Numbers are based on annualized 2016Q1 lending data.
Source: Company websites, Bloomberg, Lend Academy, Federal Reserve, FRBNY estimates.

Cumulative MPL* Origination Volume by Lending Segment

Based on $50 Billion Cumulative Origination Volume



Source: FRBNY, company websites, as of April 2016. Cumulative data begins in 2009. Figures are estimates due to intermittent reports of origination volumes. Firms included: Avant, CANCapital, CircleBack Lending, CommonBond, Credibility Capital, Dealstruck, Earnest, Groundfloor, Kabbage, Lending Club, LendingHome, LendKey, Marlette Funding, OnDeck, Patch of Land, Prosper, RealtyMogul, SocialFinance, Upstart. *Marketplace Lending (MPL)

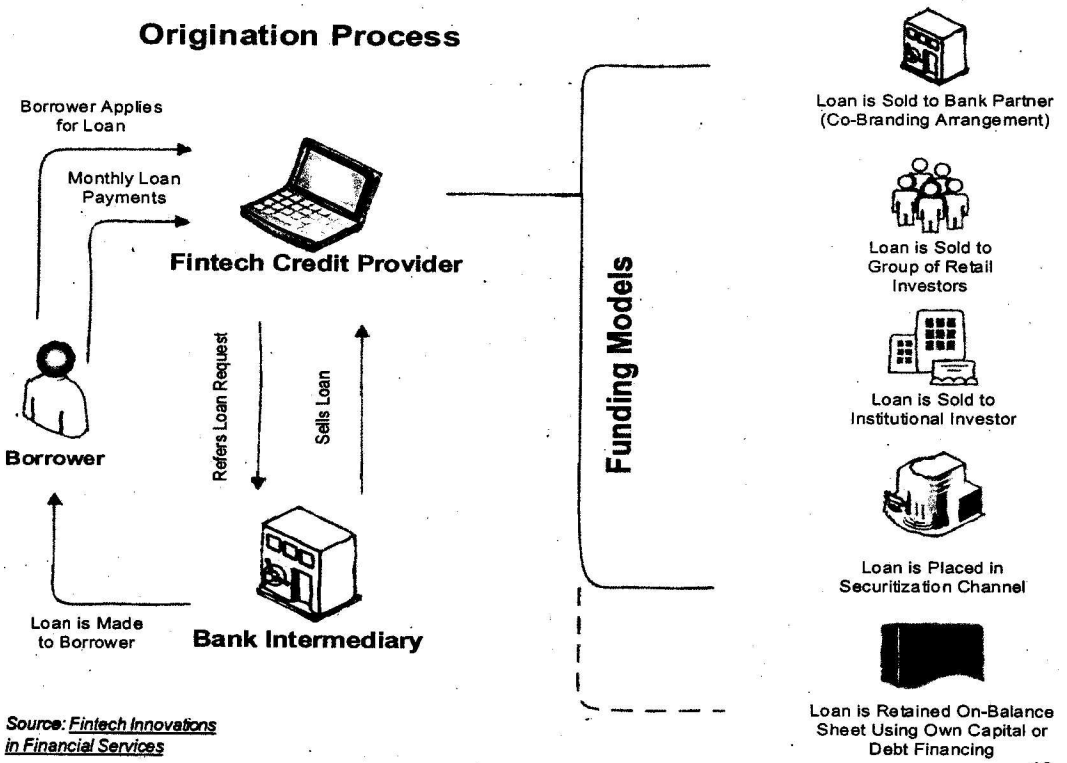
- Based on annualized 1Q16 originations, the top four alternative lenders are on pace to represent only about 3 percent of total consumer credit in United States.

- Personal loans are primarily used for debt consolidation, credit card repayment, and home improvement.
- The majority of consumer loans are made to prime or near-prime borrowers.

Bank Engagements with ALs

- **Traditional AL business model** – Banks originate loans (funding from individuals/institutional investors).
- **Partnerships** – Banks provide referrals, whole loan purchases, white labeling/cobranding of AL lending platform, and securitization services.
- **Funding** – Banks fund ALs through credit extensions, whole loan purchases, and equity investments.
- **Acquisitions** – Banks acquire an AL that becomes a primary business line unit, such as an online consumer lending unit.
- **Incubators** – Banks provide workspace, seed funding, mentoring, training, and other related support for startup entrepreneurs.

Business Model Example



Source: Fintech Innovations in Financial Services

Alternative Lenders Face Hurdles

- "Goldman, Jefferies Put LendingClub Deals on Hold"

Wall Street Journal, May 10, 2016

- "LendingClub CEO Fired Over Faulty Loans"

Wall Street Journal, May 9, 2016

- "Prosper Marketplace to Cut Jobs and Shuffle Executives"

Wall Street Journal, May 3, 2016

- "OnDeck Losses Grow as Lender Sells Fewer Loans"

Wall Street Journal, May 2, 2016

- "Fintech Lenders Dial Back Marketing in Response to Softer Investor Demand"

Wall Street Journal, April 10, 2016

Alternative Lending: New Risks and Challenges

- Data movement:
  - Data aggregators – Customer permissions, screen scraping, authentication methods, and use of APIs → ZW: via APIs change/transfer Bank (account)
  - Data ownership, security, and privacy
- Data usage:
  - Nontraditional data sources – What is used? How is it used? Is it accurate?
  - Impact of algorithms, machine learning, and artificial intelligence
- Market transparency:
  - Not all lenders are reporting to credit reporting agencies.
  - Transparency of algorithms/underwriting models:
    - Consumer ability to understand how their behaviors impact their creditworthiness
    - Inability for banks and investors to fully understand the impact of algorithms and models through the entire credit cycle
- New business models:
  - Chartering and oversight
  - Regulatory uncertainty
  - Regulatory innovation hub
  - Investor redlining

Alternative Lending: Existing Risks and Challenges

- Credit and business model risks:
  - Customer sourcing and risk for adverse selection
  - Ability to maintain strong growth and associated pressures to do so
  - Loan performance and risk retention
  - Fintech funding challenges – Balance sheet and loans
  - Untested credit models and data algorithms
  - Opaque underwriting practices
    impenetrable
- Compliance and operational risks:
  - Consumer protection – Fair lending, unfair and deceptive
  - Small business protection – Need for similar consumer protection safeguards?
  - BSA/AML, Know Your Customer, and fraud
  - Third-party risk management
  - New technologies and partnerships
  - Regulatory costs
- Reputation risk:
  - "WebBank: The Ugly Duckling Behind the San Bernardino Loan" – *Financial Times*, December 11, 2015
- Strategic risk:
  - What missteps might banks make as they adjust their strategic plans to deal with this competitive threat?

ALs: Fair Lending – Potential Disparate Impact Practices

- Disparate impact – When a lender applies a racially or otherwise neutral policy or practice equally to all credit applicants, but the policy or practice disproportionately excludes or burdens certain persons on a prohibited basis, the policy or practice is described as having a "disparate impact."
- Different loan terms – Applying via the fintech firm's website vs. branch walk-in

using social media: big issue in U.S.

who can use?
what can be utilized?
and how?

Summary: Federal Reserve - Key Points of Consideration

- Fintech covers many types of financial products and services
  - Understand how financial institutions are already engaging or plan to engage in fintech activities
  - Think beyond innovation as being good or bad. Many products could be beneficial and addressing an unmet need.
  - Understand emerging views and public statements from various regulators
  - How do we address risks and concerns, while still allowing opportunities to foster?

Appendix

List of Companies in Key Fintech Segment

Credit	Savings, Investments, Financial Planning	Digital Payments	Blockchain & Virtual Currency	Data and Technology Ecosystem
• Lending Club • Prosper • SoFi • Kabbage • OnDeck • Affirm • Ascend • PayPal Working Capital • Square Capital	• Betterment • Wealthfront • Future Advisor • Personal Capital • Digit • Acorns • Even	• Paypal (Venmo, Xoom) • Google • Apple Pay • Seemless • Stripe • Square • MCX • Dwolla • Yapstone	• The Linux Foundation • R3CEV • Digital Asset Holdings • Bitcoin • Coinbase • Ripple • Chain	• Plaid • AlphaSense • Dataminr • BillGuard • Yodlee

Additional Resources

Federal Reserve

- FRB Governor Lael Brainard, April 2016 – The Use of Distributed Ledger Technologies in Payment, Clearing, and Settlement
- FRB Governor Lael Brainard, October 2015 – Community Banks, Small Business Credit, and Online Lending
- FRB San Francisco President John Williams, April 2016 – Fintech: The Power of the Possible and Potential Pitfalls
- FRB San Francisco Senior Vice President Teresa Curran, April 2016 – Tailoring, Fintech, and Risk Culture: The Talk of the (Community Banking) Town

Other U.S. Regulators

- CFPB – Marketplace Lending Consumer Complaints
- CFPB – Understanding Online Marketplace Lending
- FDIC – Supervisory Insights Marketplace Lending Article
- OCC – Supporting Responsible Innovation in the Federal Banking System: An OCC Perspective
- U.S. Treasury – Opportunities and Challenges in Online Marketplace Lending
- California Department of Business Oversight – Survey of Online Consumer and Small Business Financing Companies

Industry Self-Regulation

- Small Business Borrowers' Bill of Rights
- Marketplace Lending Association (newly formed trade association)
- Innovative Lending Platform Association (newly formed trade association)

IT Risk: Payment Systems and Operations

Agenda – Purpose of Presentation

- Describe why high volume and payments system transactions generate operational risk.
- Identify components of internal controls processes that effectively cover products, activities, processes, and systems for operational risk.
- Recognize sound controls for front end, middle, and back office processes.
- Recognize the roles Financial Market Infrastructures (FMIs) play in the business activities of a firm and the risks associated with doing business with them.

Primary Types of Payment Systems

Payment System	Summary
Retail	Retail payments usually involve transactions between two consumers, between consumers and businesses, or between two businesses. Given the consumer-oriented nature of these payments, they tend to generate a large volume of transactions each day, though the dollar amount of each transaction is relatively small.
Wholesale	Wholesale payments typically take place to support domestic and international commercial activities, such as commercial loan and real estate transactions and financial market-related activities like corporate and governance securities and foreign exchange transactions. Wholesale payments, thus, tend to be large in value per transaction but small in terms of the volume of transactions generated daily in comparison to retail ones.

Retail Payment Instruments

- Payment instruments for retail purchases of goods and services are used to:
  - receive payments as a merchant;
  - pay one-time and recurring bills;
  - move payments between a consumer's account or the account of another consumer; and
  - access funds to make a payment, such as receiving cash from an automated teller machine (ATM) or with a credit card advance.

Retail Payment Instruments

- Retail payments, driven by technology innovations and customer demands for faster payments, include:
  - Automated Clearing House (ACH)
  - Credit Card
  - Debit Card
  - Electronic Instruments (Mobile and Internet)

Non Bank Third Parties

in U.S. ⇒ not protected

- Increased participation of nonbank third parties
  - Forces innovation
  - Lengthens transaction chain
  - Drives strategic partnerships
  - Requires diligent oversight
  - Necessitates fraud detection evolution

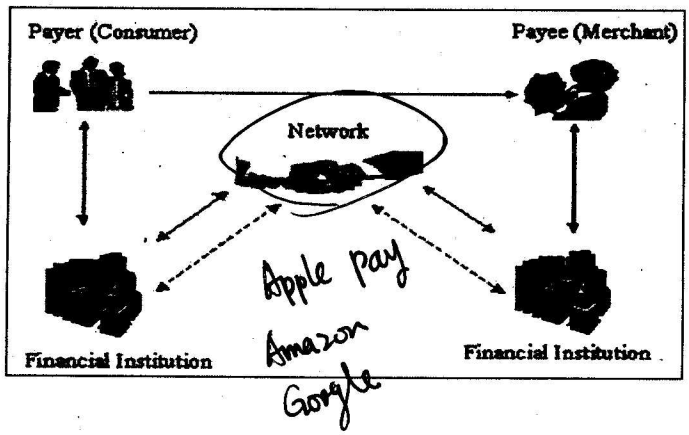
Questions:
Buy your data [卖你的]
Q. fiber bank [光纤]

Governance

- Governance process for evaluating risks introduced with new payment instruments should consider:
  - Deployment
  - Implementation
  - Use, both internally and by customers
  - Fraud detection

Clearing and Settlement

- **Clearing:** transfer and confirmation of information between the consumer and merchant
- **Settlement:** actual transfer of funds between payer and payee's financial institution



Financial Market Utilities

having many side

DTC
DCC?
SEC
OCC
CCP
} Dodd-Frank Act

process:
1. identification
2. protection
3. prediction
4. detection
5. respond
6. recovery (back-up system)

- Multilateral systems that provide the infrastructure for:
  - Transferring
  - Clearing
  - Settling payments, securities, and other financial transactions
- Among financial institutions or between financial institutions and systems
- Firms were recognized as systemically important as operational failure could increase the risk of significant liquidity risk or disruption in flow of credit

paypal: 1. not supervised by bank
2. venmo payment
social payment service

Operational Risk Exposure

Exposure	Summary
Fraudulent transaction	[redacted]
Interconnectivity	The complex interconnections between systems and vendors in the financial services industry also increase operational risk. It is difficult to find a firm that is not somehow connected to a shared service provider or other financial entities, as the nature of payment systems is to allow for settlement to take place across accounts and financial organizations. Even so, with greater connectivity, there is the risk that a single point of failure or malicious threat could have a compound impact.
Technology innovations	[redacted]

Operational Risk Exposure

Exposure	Summary
Nonbank entities	Fueled by the latest technologies and customers' demand for new financial products and services, some nonbank entities serve as competitors while others have products that maybe used or acquired by financial institutions or competing service providers. Regulatory scrutiny over such entities is significantly different. Consequently, the ability for these entities to offer a stable, secure product or handle customer information in a compliant manner may pose a direct or indirect risk to payment systems.
Cybersecurity	Threats to cybersecurity continue to build as attacks evolve and the introduction of more electronic payment channels offer additional access points to be exploited. System availability has grown in importance, as more transactions and real time information is expected; thus, the threat of cybersecurity also poses a risk that a system or information will not be available or accurate when needed.
Process failures	Processes resulting in limitations of system automation or errors in human controls can also be a significant source of operational risk, either by allowing fraud or malicious actions to be taken or unintentional errors and omissions to occur.

B.C.C.P

Supervisory Considerations

the settlement co. will pay the big member for the cost, settlement fault

Even ... could has the ability to pay the lost, how if the lost get huge ?

- Front-end Controls
- Back-end Controls
- Disaster Recovery and Business Continuity
- Information Security
- Vendor Management
- New Product Risk Assessment
- Audit Plans
- Risk Reporting
- Cybersecurity Threats

Business Resiliency – Sound Practices Paper

The four broad practices identified for core clearing and settlement organizations play a significant role in critical financial markets. They include:

- identifying clearing and settlement activities in support of critical financial markets;
- determining appropriate recovery and resumption objectives for clearing and settlement activities in support of critical markets;
- maintaining sufficient geographically dispersed resources to meet recovery and resumption objectives; and
- routinely using or testing recovery and resumption arrangements.

1. Pro: efficent, safe

2. Con: long operation rist

Payment Systems Evolution - BlockChain