FinTech Risk Management
Discussion Agenda

• What is FinTech? – A basic orientation to its intent, impact, and application
• What's the risk? – Risk management concerns for incorporating FinTech solutions
• What can be done? – Leading practices for managing FinTech operational and relationship risk
• Questions?
What is FinTech?
FinTech – A refined understanding of a broad concept

- FinTech 101: "Financial" + "Technology" = "FinTech"
- No correct definition, but everyone agrees FinTech will be impactful
- FinTech evolving as new technologies continue to emerge (Machine Learning, AI, Open API)
- Shifting industry paradigm may redefine banking (Banking as a Service, Banking as a Platform)
- Key consideration: What approaches can organizations take to realize the opportunity of FinTech while being mindful of its concerns?

"Bankers and Supervisors alike need to learn more about Fintech and develop appropriate strategies to capitalize on its benefits and mitigate its risks…" - Teresa Curran, Former SVP SF Fed
Overview of the FinTech solutions industry

• Some solutions may be supportive while others are disruptive

• A trillion dollar industry, anticipating high growth

• Significant competitive headwind for traditional banking services

• Big banks are focusing on homegrown solutions

• FinTech is not just the ream of startups, major tech firms hold a majority of market share
The evolving promise and value of Fintech solutions

• Origin story: From lower costs to a better customer relationship

• FinTech evolution: Banking made better, through the wonders of technology...

• A nascent industry: Fintech is still relatively young and new solutions continue to be developed

• Brick and mortar to screens and servers: FinTech may accelerate the rate of change associated with the digitization of branch transformation

"Everything that is happening in Finance is digitized. So pretty much every industry, every function in every industry, has a huge element that's driven by information technology…"
-- Satya Nadella, CEO Microsoft
Fintech common locations and delivery modes

- No longer just the back office, FinTech now spans the financial value chain
- From innovation to disruption: will Fintech solutions be friend, foe, or maybe both?
- Bank transformation: Evolving to enhance collaboration as a plan for survival
- Key consideration: What should banking organizations be concerned with regarding FinTech?

"FinTech touches many sectors and it offers some exciting ways to modernize the banking industry. At the end of the day, it’s about efficient market function and protecting the consumer…"  
~Patrick Harker, President, Philadelphia Federal Reserve Bank"
What's the risk?
Risk management – Overview of a critical function

• Risk management 101: Mitigation not elimination

• Risk appetite or tolerance: A critical exercise in understanding acceptable risks

• Enterprise risk management: A comprehensive approach to organizational risk management

• Key consideration: How does an organization gain comfort with incorporating FinTech solutions and whether they will be managed appropriately?
Internal operations and third party risk considerations

- With new processes and solutions comes decreased process maturity and increases to existing operational risk
- Greater integration and model driven solutions will increase the potential for biases and systematic risk
- Greater integration will compound vendor third party risk and will place greater emphasis on active management and strength of third party relationships
- How will the incorporation of FinTech impact the customer?

Fintech has the potential to transform the way that financial services are delivered and designed as well as the underlying processes of payments, clearing, and settlement…”
~Lael Brainard, Fed Board of Governors
IT and application security considerations

• Contagion risk will become more relevant
• Vendors may take significantly different approach to cyber and data security
• Data models and systems may not be suited for non-traditional FinTech data.
• Integrated solutions will place greater burdens on existing IT infrastructure (i.e. Banking as a Service/Banking as a Platform)
• Process intermediaries can be opportune targets for cybersecurity threats
HR and corporate governance considerations

- Clash of the cultures: Organizational objectives and values may not mesh with solutions providers...

- Governance structures may be poorly staffed and structure to provide oversight

- Fintech solutions may be "silhoed' within certain departments or functions

- Existing staff may not have the requisite skills or expertise needed to adapt new solutions

- Efficiency gains perhaps, but compliance risk isn't going away and may get worse.

"Financial services firms must pair innovative services with a strong compliance culture and knowledge of legal and compliance guiderails..." ~ Lael Brainard, Federal Reserve Governor
Assessing FinTech's value and strategic fit

- FinTech not a patch: Evaluate solutions strategic alignment and fit with people, process, and existing technology
- Perform a comprehensive cost benefit analysis, emphasizing sustainability
- Budget for initial redundancy and a trial period as new systems are brought online
- Not shiny new toy: Don't neglect how exciting solutions might impact key risk areas such as strategic or reputational risk
What can be done?
Leading practices for evaluating FinTech providers and solutions

• Approach partner vendor vetting process as though they were an acquisition and formalize relationships

• Carefully assess the maturity of a FinTech solution and stage of its lifecycle

• Develop formal vetting mechanisms and process to level the playing field and to ensure consistent evaluation

• Keep the customer in mind: Increasing mechanisms to ensure protection of customer data privacy
IT security considerations

• Bring a bigger umbrella: Ensure that FinTech processes and solutions are appropriately supported by robust IT infrastructure

• Utilize the opportunity to assess data integrity and further increase automation of manual processes

• Ensure disaster recovery and business continuity plans are updated and robust

• Reevaluate system architecture to consider process dependence and potential contagion concerns

• Incorporate advanced analytics and assessment capabilities (data analytics)
## IT security considerations (API specific)

<table>
<thead>
<tr>
<th>API Vulnerability</th>
<th>Control</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Injection</strong></td>
<td>• Follow secure coding practices</td>
</tr>
<tr>
<td><strong>Broken Authentication and Session</strong></td>
<td>• Follow secure coding practices</td>
</tr>
<tr>
<td>Management</td>
<td>• Apply/use native web framework handers</td>
</tr>
<tr>
<td><strong>Cross-Sites Scripting</strong></td>
<td>• Follow secure coding practices</td>
</tr>
<tr>
<td><strong>Insecure Direct Object References</strong></td>
<td>• Properly sanitize input (client side and server side)</td>
</tr>
<tr>
<td><strong>Security Misconfigurations</strong></td>
<td>• Implement RBAC at a granular level</td>
</tr>
<tr>
<td><strong>Sensitive Data Exposure</strong></td>
<td>• Enforce strong encryption</td>
</tr>
<tr>
<td><strong>Missing Function Level Access Controls</strong></td>
<td>• Set access default to denial</td>
</tr>
<tr>
<td></td>
<td>• Block all web file types</td>
</tr>
<tr>
<td></td>
<td>• Restrict access to all web files</td>
</tr>
</tbody>
</table>
## IT security considerations (API specific)

<table>
<thead>
<tr>
<th>API Vulnerability</th>
<th>Control</th>
</tr>
</thead>
</table>
| **Cross-Site Request Forgery (CSRF)**      | • Use an API-key based authentication  
• Allow your API to accept UI authentication, like the SESSIONID cookie, but require that API calls made with that form of authentication have additional security checks on them. |
| **Vulnerable Components**                  | • Stay updated                                                                                                                                 |
| **Invalidated Redirects or Forwards**      | • Avoid using redirects and forwards  
• Don’t allow the url as user input for the destination  
• Map destinations as a value and use server side validation to check that value |
Regulation – Dealing with every banker's best friend

• Taking a proactive approach: Planning ahead for future regulatory scrutiny integration and expectations of access will come with greater scrutiny

• Regulatory strategy: Establish frameworks for addressing regulatory concerns and building trust and confidence

• Don't pass the buck: Maintain thorough understanding of FinTech partners regulatory requirements and challenges

• Look forward to the future: RegTech and potential for technology compliance solutions

"The challenge for policymakers is to ensure that Fintech develops in a way that maximizes the opportunities and minimizes the risks for society..."
~Mark Carney (Bank of England Governor)
Enterprise risk management and governance leading practices

• Give risk a seat at the table: Fully integrate risk management functions in strategic planning exercises

• Develop organizational groups that are structured to be nimble and responsive to address emergent risks

• Pair innovative processes with a compliance culture that values risk management

• Management develops detailed standards and metrics to evaluate FinTech performance emphasizing sustainability
Incorporating new risk management function techniques

• Majority of major banks seeking efficiency and optimization in risk management function
• Bigger risk management presence without increased cost of compliance
• Risk management will increasingly inform business strategy
• Advanced risk analytics directly linked to implementing digital and new business models
• Wrap up: Risk Management itself will leverage FinTech as it seeks to optimize, increase efficiency, and greater inform strategic goals
Any questions???
Thank you for attending

Visit us online at:

www.GrantThornton.com
twitter.com/GrantThorntonUS
linkd.in/GrantThorntonUS