Digital Banking Poses Challenges for Third-Party Risk Management

Digital banking is a disruptive trend growing in the banking industry across the world. Simply put, it includes banking services provided primarily or wholly through digital or electronic means.

Industry Overview

There are many players in the market that would consider themselves "digital banks." However, by strict definition, a bank has to be chartered by regulators in most countries. Digital banks typically fall within two categories (others are considered bank partners):

1. Established banking institutions that either extend their existing services through digital channels where possible or build tailor-made services to customers online (e.g., Marcus by Goldman Sachs)
2. Startup organizations granted a banking license (i.e., neobanks) that provide services in digital-only, mobile-first channels (e.g., Monzo in the United Kingdom)

This new trend is accompanied by the unprecedented scale and depth of banking institutions working with third parties, posing new challenges to the third-party risk management approach banks traditionally employ.

Common Third-Party Relationships in Digital Banking

Though some exist in traditional banking business, a number of third-party relationships are typical in the digital banking context:

- **Dominant Internet platforms**—These platforms are usually not oriented toward becoming regulated financial institutions. Instead, they work with banks to embed banking services into their platforms to achieve greater synergy and monetization within their ecosystems. These Internet platforms allow banks to access unbanked or underbanked customers and offer alternative insight into risk management for customers. An example would be credit lines to Amazon merchants offered with Goldman Sachs.[1]
- **Specialized business to consumer (B2C) financial technology (fintech) platforms**—These are usually not licensed banks, but they can directly serve individual customers or small businesses with highly customized solutions that include some banking service components (e.g., lending and payment processing). They can target customers' unmet financial needs in niche

Maosen Cai, CISA, CIA, FRM
Is an audit analytics lead at one of the biggest digital banks in China. He drives innovative analytic solutions into business and risk dimensions to support governance of the bank. Prior to that, he was a manager in risk advisory practice at Deloitte China.

Han Yan, CISA, CIA, FRM
Is an audit senior manager at one of the biggest digital banks in China. He oversees internal audit and governance programs within the bank. Prior to that, he was a manager in enterprise risk services at Deloitte China.

use cases and move nimbly to address them. In some cases, they partner with incumbent banks to navigate regulatory hurdles involved with services such as taking deposits and underwriting loans.

- **Digital banking solution providers**—The technology prerequisite for digital banking is different from that hosted by incumbent banks in-house. This gives rise to organizations that specialize in developing technology solutions to enable digital banking, also known as Banking as a Service (BaaS). Instead of having to maintain full-stack legacy technologies, banks can now focus on their unique advantage and be agile in responding to customer needs, leveraging out-of-box application programming interfaces (APIs) and solutions available in the market and the cloud.
- **Data providers/facilitators**—The inherent lack of physical reach to customers pushes digital banks to pursue alternative data sources such as for credit assessment, customer identity verification and antifraud. This is usually available through open APIs facilitated by third-party providers that are then responsible for connecting to different data sources such as customer information in other banks, credit reports and identification data.
- **Other financial institutions**—On the demand side, digital banks may have revolutionized how customer needs are fulfilled and how services are delivered; however, on the supply side, they still have to work with existing financial institutions, especially for services related to financial infrastructure such as interbank transactions and payment processing. They may also partner with other financial service providers such as insurers and securities brokers as digital banks endeavor to be the one-stop-shop for customers' financial needs.

Risk Arising From Third-Party Relationships

Third-party engagement affects all levels of digital banking from operations support to the core business. If not managed properly, third-party relationships can potentially cause a contagion effect in all major risk domains, particularly the following.

Strategic Risk: The Indispensable Dependency
The last decade of booming Internet-based economy ended with a few dominant players growing from different vertical segments into massive digital platforms connecting billions of users (e.g., Facebook,[2] Tencent). These platforms offer unique advantages and opportunities for digital banks but with an unbalanced position of bargaining power. For Internet giants, financial services provided by digital banks are intended to expand customer footprints within their own digital ecosystems while taking the lion's share of profits from those services. Their ultimate goal is to reinforce their ecosystem dominance and, in doing so, they tend to play a marketplace role among diverse groups of financial service providers. For digital-only banks, the unparalleled dependency on third-party Internet platforms is sometimes unavoidable and uncontrollable. Furthermore, competing Internet giants may force their partner banks to take sides for an exclusive cooperation relationship.

> "THIRD-PARTY ENGAGEMENT AFFECTS ALL LEVELS OF DIGITAL BANKING FROM OPERATIONS SUPPORT TO THE CORE BUSINESS."

Credit Risk: New Frontiers of the Old Game
A significant portion of digital-banking services via third-party Internet platforms is online lending, commonly in the form of loans or credit lines granted to customers on these platforms. Retail-credit risk management traditionally focuses on assessing the borrower, but digital lenders would have to include the partnering platform as an ongoing risk variable. Such risk may include:

- Each Internet platform has target customer groups subject to sporadic changes based on market conditions. If the change is beyond the expectations of digital banks, it might subsequently nullify risk assumptions and variables previously built, and prevent existing risk models/algorithms from working as intended.
- The platform itself operates under different incentives than the digital lenders and may sometimes push for undesirable customer

actions from a risk perspective. For instance, customers may be lured by misinterpreted marketing to opt into buy now pay later (BNPL) offers (i.e., installment loans) for unaffordable purchases, only to dispute repayment later in the collection process.

- Due to technology constraints or user experience considerations, not all due validation can be performed to facilitate credit risk assessment, or all required variables may not be collected on the third-party platform.

Compliance Risk: Innovation in a Legacy World

The regulation landscape is evolving with the boom of digital banking, but it is not always in sync. In fact, desynchronization is the root of many compliance issues facing digital banks, and third-party relationships are no exception. On one hand, regulation over third-party relationships is based on past decades of banking experience and multiple financial innovation failures turning into chaos. Digital banks running on innovative business models with third parties might seem vulnerable from a regulatory perspective, not to mention the resistance from established banks to safeguard their interests aligned with existing regulation. On the other hand, digital banks should not fear regulation. Digital banking or financial technology at large can be nurtured positively for financial inclusion, but it can also be abused because of greed. For example, peer-to-peer (P2P) lending enabled by digital platforms once boomed in China amid little or no regulation,[3] but as these platforms unduly issued loans from individual investors' money instead of from their own pocket, large-scale defaults emerged, resulting in the almost entire collapse of the P2P lending sector.

Cyberrisk: The Extended Enterprise

In a digitally interconnected world, the cybersecurity strength of any single player is not measured by its own defense but by the weakest link in the broader ecosystem. Likewise, digital banks need to consider their partners' cybersecurity to an equal degree as their own. Such threats have never gone far: In September 2017, Equifax, a major credit bureau in the United States, announced a data breach in which hackers were able to access the private information of 147 million consumers.[4] This included names, social security numbers, dates of birth, credit card numbers and even driver's license numbers. Further investigation revealed that Equifax was aware of the system's vulnerability before it was exploited but failed to install the necessary patches. It was not a digital bank, but the data breach illustrates the cybersecurity risk that arises from ecosystem partners.

> "OPPORTUNITIES AND CHALLENGES FOR THIRD-PARTY RELATIONSHIPS CONFRONTING DIGITAL BANKS CALL FOR A MORE HOLISTIC AND PRAGMATIC APPROACH."

The Holistic Approach to Third-Party Risk in the Digital Banking Age

Opportunities and challenges for third-party relationships confronting digital banks call for a more holistic and pragmatic approach, as summarized in three guiding principles:

1. **Be strategically pragmatic**—Third-party relationships are, ultimately, a process of achieving power equilibrium between digital banks and their third parties. The fundamental question is: How indispensable is one to the other? Digital bank leadership must strategically consider its competitive advantage toward each third party and strive to become an integral component of that third party's core business.
2. **Continuously prioritize**—Banking is inherently a business of balancing risk and return, and so is the third-party relationship. For example, the upside of a digital bank's reliance on third-party Internet platforms is faster time to market and scalability. However, it is important to determine when the risk should be prioritized over its return and *vice versa*. One particular cause of concern is economic cyclicality (i.e., existing dominant Internet players are the result of early digitalization of certain industries and sectors and may saturate earlier than later adopters). Digital banks looking to partner with these platforms must continuously weigh and make a trade-off between emerging opportunities and corresponding risk.

> THIRD-PARTY RISK SHOULD NEVER BE MANAGED IN A SILO, BUT RATHER, INTEGRATED INTO OTHER DOMAINS OF RISK MANAGEMENT BOTH AS AN IMPORTANT INGREDIENT AND A NATURAL EXTENSION. FOR EXAMPLE, THE DIGITAL BANK'S COMPLIANCE RISK.

3. **Manage change as the only constant**—Market dynamics are evolving fast, even within digital banks. Digital banking products and services have to constantly stand up in the market. If proved undesirable, they may pivot or even cease to exist. Third-party relationships should evolve to reflect these constantly changing business cases and conditions on an agile basis.

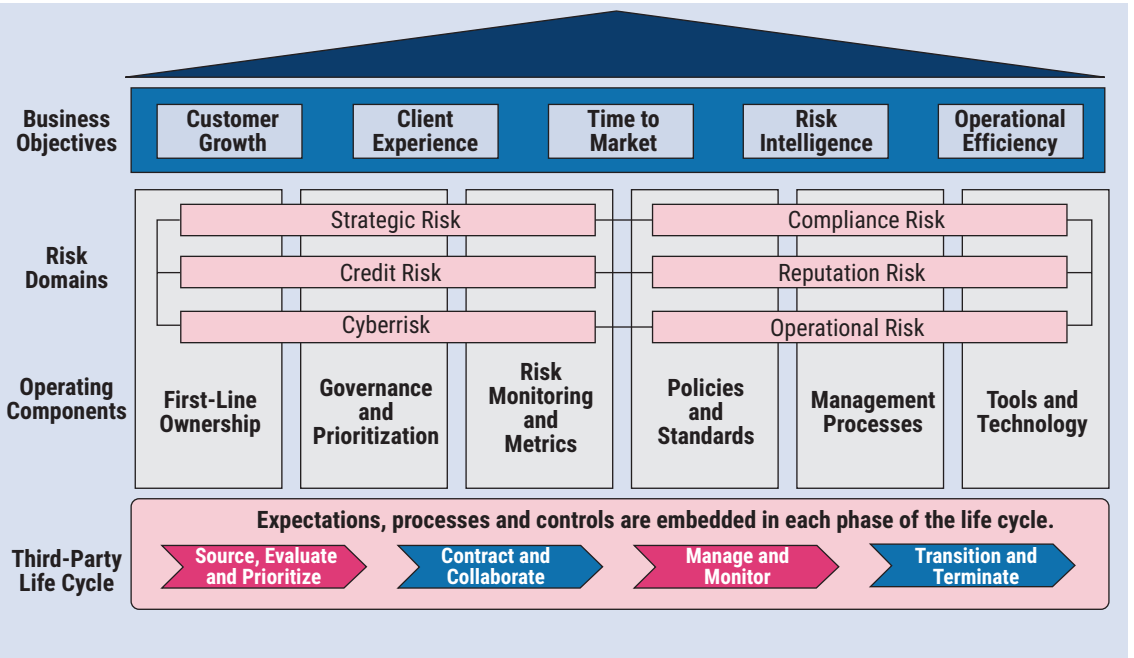
Accordingly, **figure 1** proposes a framework for managing third-party risk from the perspective of digital banks. This framework can be elaborated on in four dimensions: business objectives, risk domains, operating components and life cycle management.

Business Objectives

Managing any third-party relationship has to start with the business objectives for using it. Not all business objectives are equal; some will override and dictate the digital bank's overall strategy across different domains of risk related to third parties, for example:

- If customer growth is the top priority for a digital bank, the bank may offer more favorable terms and flexibility to third-party platforms with larger customer bases otherwise unreachable by itself. Such differentiation mandates the digital bank to retrofit its credit risk strategy, including credit scoring of incremental customer groups and individual risk policies.
- If operation efficiency is the preferred objective of a digital bank, it may standardize its approach, processes and metrics across different third parties and reduce flexibility specific to any single third-party relationship. In return, the bigger Internet platforms would be less incentivized to partner with this digital bank, resulting in revenue/customer targets not achieved in full potential.

Figure 1—Third-Party Risk Management for Digital Banks



Risk Domains

Third-party risk should never be managed in a silo, but rather, integrated into other domains of risk management both as an important ingredient and a natural extension. For example, the digital bank's compliance risk management function should watch for negative news and inappropriate practices of its major third parties. The cyberrisk team should go the extra mile looking for vulnerabilities and incidents arising from these ecosystem partners.

Operating Components

The operating model for third-party risk management consists of the following interrelated components:

- **First-line ownership**—With third-party relationships now being integral to digital banks, they should be part of the first-line manager's responsibility. These managers should be accountable for the quality and compliance metrics of third-party relationships in day-to-day business.
- **Governance and prioritization**—Digital bank leadership should not rest once a third-party risk management framework is established. Since the industry dynamics progress rapidly, it is imperative to have an ongoing mechanism that is effectively carried out to oversee how existing risk management practices perform in response. The governance mechanism should also be able to rigorously prioritize new opportunities and risk areas when they emerge.
- **Risk monitoring and metrics**—Like other risk management processes, third-party risk management requires dedicated risk monitoring efforts and metrics, which support digital bank management teams in reviewing previous decisions and formulating new ones accordingly. This can include positive performance metrics (e.g., how a third party lives up to its service-level commitments) and negative quality metrics (e.g., customer complaints related to individual third parties).
- **Policy, process and technology**—As foundational elements, policies and standards define management expectations for third-party risk management. These are facilitated by a set of processes and technology tools to navigate risk through the life cycle.

Third-Party Life Cycle

There is a life cycle for any third-party relationship regardless of its duration. Expectations, processes and controls that should be put in place seamlessly within these life cycles include:

- **Source, evaluate and prioritize**—When sourcing specific categories of partnerships, business objectives should be prioritized to lay out management expectations for selecting third parties. No third party is perfect, but the ones selected should be defined along with risk-mitigating controls to be implemented in later stages of the relationship.
- **Contract and collaborate**—Besides general business terms, digital banks should also consider internal policies and standards from different risk domains for integration into contracting obligations with third parties. This would help ensure collaboration with third parties to create a closed-loop management cycle of all risk domains.
- **Manage and monitor**—Throughout the relationship, third parties should be monitored to ensure that they adhere to strategic goals and contracting commitments and to justify any management actions required by digital banks.
- **Transition and terminate**—Third-party relationships might undergo changes and eventually termination when the planned business case change is invalidated or the expected outcomes are not realized. As such, transition arrangements for pullout of either party should be defined in the beginning and exercised regularly. These arrangements should cover areas such as data, client relationships and intellectual property.

> "SOUND THIRD-PARTY RISK MANAGEMENT IS THE NEW CORE COMPETENCY FOR ALL BANKS."

Enjoying this article?

- Read *Bridging the Digital Risk Gap. www.isaca.org/digital-risk-gap*
- Learn more about, discuss and collaborate on risk management in ISACA's Online Forums. *https://engage.isaca.org/onlineforums*

Conclusion

The end state for digital banking is yet to be seen. Whatever happens, banking services will always be needed even though bank branches may be gone. More and more banking services are embedded into people's everyday lives. That is where third-party relationships come in and why they will remain vital to the continued prosperity of digital banking in the foreseeable future. Sound third-party risk management is the new core competency for all banks, whether it is a digital bank looking to continue its success or a traditional bank looking to revive itself in the new age.

Endnotes

1 Son, H.; "Amazon Unveils Small Business Credit Line With Goldman in Latest Tie-Up Between Tech and Wall Street," CNBC, 10 June 2020, *https://www.cnbc.com/2020/06/10/amazon-and-goldman-sachs-unveils-small-business-credit-lines-up-to-1-million.html*

2 Facebook, *Facebook Q1 2020 Results*, USA, 2020, *https://s21.q4cdn.com/399680738/files/doc_financials/2020/q1/Q1-2020-FB-Earnings-Presentation.pdf*

3 Liu, J.; "The Dramatic Rise and Fall of Online P2P Lending in China," *TechCrunch*, 1 August 2018, *https://techcrunch.com/2018/08/01/the-dramatic-rise-and-fall-of-online-p2p-lending-in-china/*

4 Leonhardt, M.; "Equifax to Pay $700 Million for Massive Data Breach. Here's What You Need to Know About Getting a Cut," CNBC, 22 July 2019, *https://www.cnbc.com/2019/07/22/what-you-need-to-know-equifax-data-breach-700-million-settlement.html*