CHALMERS
UNIVERSITY OF TECHNOLOGY

Managing partnerships for payment product distribution

How financial technology companies can balance opportunities and risks

Master's thesis in Management and Economics of Innovation

KLARA PILHALL

DEPARTMENT OF TECHNOLOGY MANAGEMENT AND ECONOMICS
DIVISION OF INNOVATION AND R&D MANAGEMENT

CHALMERS UNIVERSITY OF TECHNOLOGY
Gothenburg, Sweden 2023
www.chalmers.se
Report No. E2023:011

REPORT NO. E2023:011

Managing partnerships for payment product distribution

How financial technology companies can balance opportunities and risks

KLARA PILHALL

Department of Technology Management and Economics
Division of Innovation and R&D Management
CHALMERS UNIVERSITY OF TECHNOLOGY
Gothenburg, Sweden 2023

Managing partnerships for payment product distribution
How financial technology companies can manage opportunities and risks
KLARA PILHALL

Report no. E2023:011
Department of Technology Management and Economics
Chalmers University of Technology
SE-412 96 Göteborg
Sweden
Telephone +46 (0)31-772 1000

Gothenburg, Sweden 2023

Managing partnerships for payment product distribution
How financial technology companies can balance opportunities and risks

KLARA PILHALL

Department of Technology Management and Economics
Chalmers University of Technology

Abstract

Driven partly by the introduction of financial technology (fintech), the global payment industry has undergone a rapid transformation during the past decades toward digital solutions and online payments. Along with this transformation, financial crime and the challenges of efficiently managing associated risks have increased. Despite multiple competitive advantages, fintech companies face challenges related to the changing dynamics in the payment industry and increasingly need to invest in technological innovation to renew their distribution channels and make payments easier, faster, and more accessible while promoting security. At the same time, business ecosystems have increasingly emerged across sectors to address uncertainties and co-evolution, promoting business collaboration for resilience and agility in networks of strategic partnerships.

This study aims to explore how fintech companies that provide online financial services can manage risks related to financial crime when partnering with third-party actors in business ecosystems for payment product distribution. A single-case study is performed, relying on qualitative research through semi-structured interviews at the case company and applying a thematic analysis to analyze the obtained data.

The study identifies that risks related to financial crime affect fintech companies that provide online financial services in multiple ways when partnering with third-party actors in business ecosystems for payment product distribution. These effects mainly concern the increased third-party dependency on external actors and the related impact on other areas that should be considered. Moreover, the study proposes actionable solutions to manage these risks. First, measures should be implemented for alignment and agreement to promote collaboration and coordination. Second, actions could be taken to incentivize adherence to the agreed risk standards. Third, fintech companies could benefit from complementing these measures with internal mechanisms to monitor and control that partners adhere to agreed risk standards and limit the risk exposure created by their partnerships. Finally, management should be involved in risk decisions and determine a dynamic risk appetite to respond to the changing dynamics in the payment industry along with these partnerships.

Keywords: Business ecosystems, partnerships, interdependence, coordination, collaboration, payment industry, online payments, financial technology, fintech, payment product distribution, financial crime, risk management, risk appetite.

Acknowledgements

This master's thesis was conducted during the spring semester of 2023 as part of my studies in Management and Economics of Innovation at Chalmers University of Technology, Division of Innovation and R&D Management.

I would like to express my gratitude toward Lisa Winberg, my supervisor at the Division of Innovation and R&D Management, who guided and supported me throughout the work of the thesis. Her positive and encouraging attitude and the knowledge she continuously shared with me have been truly valuable. I would also like to thank Ingrid Johansson Mignon, my examiner at the Division of Innovation and R&D Management, for dedicating her time and sharing her insights with me through our nurturing discussions.

In addition, I would like to thank my supervisors at the case company with which the thesis was conducted in cooperation. Thank you for helping me arrange this study, continuously sharing your valuable knowledge, and supporting me throughout this project. Finally, I would like to sincerely thank the research participants for generously taking the time to share their insights on strategic partnerships and risk management. Without the patience and contribution of each one of you, this project would not have been possible.

Klara Pilhall
Gothenburg, May 2023

Table of Contents

List of Acronyms

Below is the list of acronyms that have been used throughout the study listed in alphabetical order:

AML	Anti-Money Laundering
API	Application Programming Interface
BCBS	Basel Committee on Banking Supervision
CDD	Customer Due Diligence
CIP	Customer Identification Program
DBE	Digital Business Ecosystem
EDD	Enhanced Due Diligence
EMV	Europay, Mastercard, Visa
Fintech	Financial Technology
KYC	Know Your Customer
PCI DSS	Payment Card Industry Data Security Standard
PSD2	Revised Payment Services Directive

List of Figures

1. Introduction

Over the past years, changing market dynamics and increasing levels of competition have created challenges for companies in most sectors (Graça & Camarinha-Matos, 2017; Li, 2009; Skog et al., 2018; Matzler et al., 2018). Along with this development, business ecosystems have increasingly emerged to address uncertainties and co-evolution among multiple actors, promoting business collaboration for resilience and agility in networks of strategic partnerships (Kapoor, 2018; Rong et al., 2015; Tsujimoto et al., 2018). At the same time, technological advances, digitalization, and the arrival of electronic commerce (e-commerce) have transformed the payment industry (Bezovski, 2016; Furst et al., 1998; Gomber et al., 2017; Gupta, 2013; Khan et al., 2017; Liu et al., 2015; Nelms et al., 2018; Sullivan, 2010). Financial technology (fintech) companies have emerged, characterized by long-term strategic advantages such as higher-quality financial services, increased efficiency, decreased costs, and improved customer satisfaction (Gomber et al., 2017; Kou et al., 2021; Leong et al., 2017). However, despite these advantages, fintech companies face challenges related to the changing dynamics in the payment industry and increasingly need to invest in technological innovation to renew their distribution channels and make payments easier, faster, and more accessible (e.g., Leong et al., 2017; Liu et al., 2015; Passi, 2018; Romānova & Kudinska, 2016). Furthermore, the development of fintech has driven significant volumes of online payments, increasing financial crime risks and creating challenges for financial companies to manage these risks (Bezovski, 2016; Giudici, 2018; Khan et al., 2017; Zetzsche et al., 2020).

This study explores how fintech companies that provide online financial services can manage risks related to financial crime when partnering with third-party actors in business ecosystems for payment product distribution. By understanding the effects of risks related to financial crime, the ambition is to develop guidelines for how fintech companies can sustainably manage their partnerships in business ecosystems considering these risks. The following chapter presents an introduction to the studied issue, the identified research gap, the aim and research questions, and the scope of the study.

1.1 Background

In recent years, business environments have been changing rapidly (Jung et al., 2020). Globalization has created challenges for businesses worldwide to cope with increasing levels of competition and market turbulence (Graça & Camarinha-Matos, 2017). Furthermore, radical digital innovation, often referred to as digital disruption, has created new opportunities for firms while demanding the reimagination of business models to navigate this transformation (Skog et al., 2018; Matzler et al., 2018). Along with this development, business environments have increasingly transformed into business ecosystems characterized by networks, interdependencies, partnerships, and value co-creation (Adner & Kapoor, 2010; Autio & Thomas, 2020; Graça & Camarinha-Matos, 2017; Hanelt et al., 2021; Hoch & Brad, 2021; Kapoor, 2018; Rong et al., 2015; Subramaniam et al., 2019). Furthermore, firms that operate in business ecosystems and successfully establish and manage their partnerships benefit from

opportunities to navigate the changing dynamics of markets and competitive environments (Clarysse et al., 2014; Zahra & Nambisan, 2012).

Driven partly by the introduction of fintech, the global payment industry has undergone a rapid transformation during the past decades toward digital solutions and online payments (Bezovski, 2016; Furst et al., 1998; Khan et al., 2017; Nelms et al., 2018; Yao et al., 2018). Besides traditional banks and credit card companies, new fintech companies offering innovative online payment services have emerged in the payment industry (Gupta, 2013; Yao et al., 2018). For instance, PayPal, Alipay, Affirm, and Apple Pay have entered the market, facilitating online payments between individuals and businesses and supporting e-commerce (Arner et al., 2022; Hayes, 2023; McKinsey & Company, 2020). The transformation of the payment industry has contributed to the creation of new business ecosystems and a shift from competition between actors to collaboration (Passi, 2018). For instance, fintech actors often operate in business ecosystems and collaborate with third parties, such as banks, payment card companies, e-commerce platforms, and payment facilitators for value co-creation and distribution of their payment products (Deloitte, 2021; Schneider, 2023; Henningsson & Hedman, 2014).

Despite multiple competitive advantages, fintech companies face challenges related to the changing dynamics in the payment industry, such as changing customer preferences, technological risks, competition threats, and regulatory compliance (Gomber et al., 2017; Leong et al., 2017; Liu et al., 2015; Romānova & Kudinska, 2016). At the same time, merchants perceive the time and effort required as the main barriers to integrating new payment methods (European Central Bank, 2022). These changing dynamics demand fintech companies to invest in technological innovation and renew their distribution channels to make payments easier, faster, and more accessible while focusing on the security of transactions (Passi, 2018). Following the increasing demand for online payments and changing customer preferences, merchants increasingly value the capacity to integrate multiple payment solutions through a single payment facilitator (European Central Bank, 2022; Global Payments, 2022; J.P. Morgan, 2021). Payment facilitators are emerging in the payment industry, allowing merchants to accept various types of payments through one integration (Gancz et al., 2022; Guthrie, n.d.). Hence, multiple financial services providers partner with third-party payment facilitators to distribute their payment products and support the integration for merchants (Apple, n.d.; Chiodo et al., 2021; PYMNTS, 2022; Stripe, n.d.). Figure 1.1 shows the relationships between merchants, payment facilitators, and financial services providers.

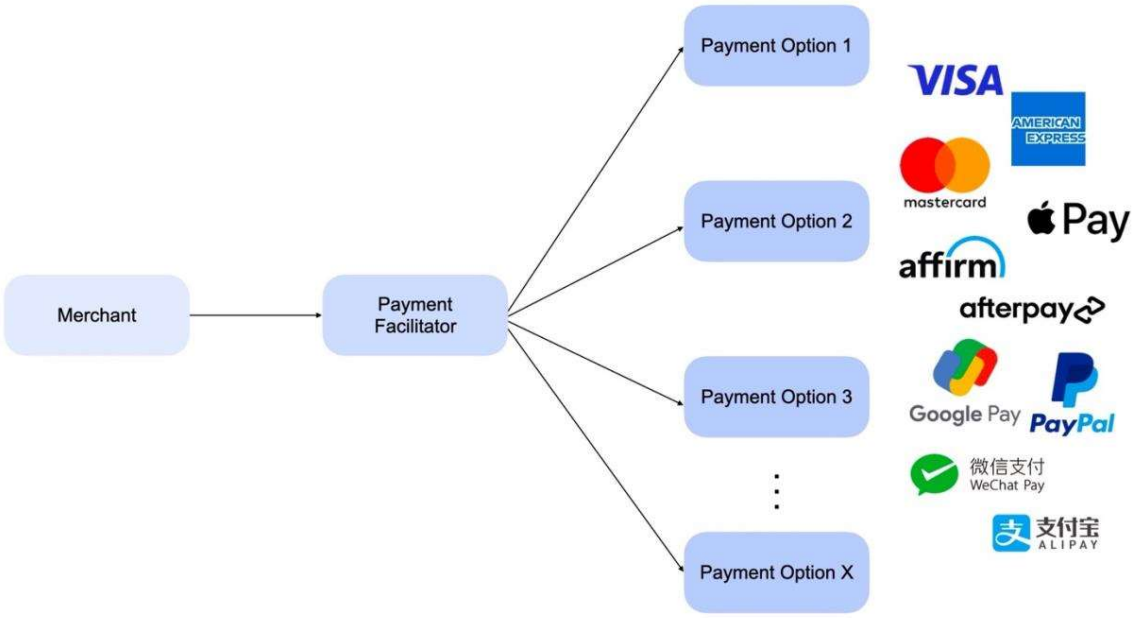

Figure 1-1: The relationships between merchants, payment facilitators, and financial services providers.

Along with the growth of e-commerce, the emergence of fintech, and the adoption of online payments, financial crime risks and the associated challenges of efficiently managing these risks have increased (Bezovski, 2016; Bolton & Hand, 2002; Hutchings & Holt, 2015; Khan et al., 2017). Fraudsters are increasingly developing applications to exploit data for identity-theft fraud, while cyber-enabled attacks are becoming more complex (Buehler, 2019). Fraud causes various risks for financial services providers, creating challenges involving financial loss, regulatory non-compliance, reputational damage, customer detriment, and decreased trust of clients (Buehler, 2019; Chapelle, 2019; Mikkelsen et al., 2022). When financial services providers partner with payment facilitators for payment product distribution, the risk assessment of merchants before they can accept payments is performed by the payment facilitator instead of the financial services provider (Soinski & Theriault, n.d.). Therefore, financial services providers increasingly expect their payment facilitator partners to have implemented strong fraud controls and anti-money laundering (AML) (Mikkelsen et al., 2022).

1.2 Research Gap

Since the emergence of fintech, substantial research has been performed explaining how traditional banks and fintech companies increasingly need to collaborate to tackle the challenges of digitalization and changing customer preferences (e.g., Acar & Çıtak, 2019; Hornuf et al., 2021; Juengerkes, 2016; Romānova & Kudinska, 2016; Takeda & Ito, 2021). Furthermore, existing literature provides evidence of how the risks of financial crime have increased along with the digitization of finance (e.g., Murinde et al., 2022; Zetzsche et al., 2020). However, there is a lack of clear explanation for how fintech companies that provide online financial services can manage risks related to financial crime when partnering with third-party actors in business ecosystems for payment product distribution. By filling these gaps in the literature, fintech companies could benefit from more informed decisions when developing

strategies for payment product distribution involving partnerships with third-party actors in business ecosystems. Furthermore, by explaining the associated risks related to financial crimes of third-party relationships and their implications, managers could more effectively evaluate the benefits of these partnerships to balance opportunities and risks, supporting strategic firm objectives.

1.3 Aim and Research Questions

This study aims to explore how fintech companies that provide online financial services can manage risks related to financial crime when partnering with third-party actors in business ecosystems for payment product distribution. To answer the aim of the study, it first needs to be understood how risks related to financial crime affect fintech companies when partnering with third-party actors in business ecosystems for payment product distribution. Second, it should be studied how these risks could be managed. Hence, the aim can be broken down into two research questions:

1. *How do risks related to financial crime affect fintech companies when partnering with third-party actors in business ecosystems for payment product distribution?*

2. *How can fintech companies manage risks related to financial crime when partnering with third-party actors in business ecosystems for payment product distribution?*

1.4 Scope

Although fintech companies exist in many different forms with different applications (Puschmann, 2017; Takeda & Ito, 2021), the work of this study will focus on fintech companies that provide online financial services and have partnerships with third-party actors for payment product distribution. Hence, partnerships with third-party actors for purposes other than payment product distribution will not be addressed. Furthermore, when evaluating the risks of these partnerships, the study will focus exclusively on risks related to financial crime.

2. Theoretical Framework

This chapter lays a theoretical foundation for the study and introduces concepts necessary to understand the studied issue. First, the chapter provides an introduction to business ecosystems and how companies increasingly adopt new organizational structures to promote business collaboration for resilience and agility in networks of strategic partnerships. The opportunities for strategically participating in business ecosystems are outlined, followed by the related challenges companies should consider and how these could be managed. Second, the payment industry is presented, including the emergence of fintech and online payments. Finally, the chapter ends with an introduction to financial crime, related risks, and theories on how these could be managed.

2.1 Business Ecosystems

Over the past years, globalization and digital disruption have transformed business landscapes (Graça & Camarinha-Matos, 2017; Skog et al., 2018; Matzler et al., 2018). Multiple studies indicate that changing market dynamics and increasing levels of competition have created challenges for companies in most sectors, demanding new business models and strategies (e.g., Graça & Camarinha-Matos, 2017; Li, 2009; Skog et al., 2018; Matzler et al., 2018). Along with these developments, business ecosystem theories have developed from dynamic supply chain theories and gained increasing attention in the field of management of technology and innovation to address uncertainties and co-evolution (Kapoor, 2018; Rong et al., 2015; Tsujimoto et al., 2018). According to Adner and Kapoor (2010), a company's competitive advantages depend on its ability to create more value than its competitors, in turn depending on its capabilities to innovate successfully. Moore (2006) highlights how companies have increasingly focused on achieving competitive advantages through continuous innovation to respond to digital disruption and changing market dynamics. However, for innovations to succeed, Moore (2006) and Adner and Kapoor (2010) underline that complementary advances must co-evolve across a system of various actors, as no single company has all the required knowledge and resources. As a result, studies emphasize how business ecosystems have emerged to coordinate innovation activities across multiple complementary actors for cooperation and jointly deliver products and services to consumers (e.g., Adner & Kapoor, 2010; Clarysse et al., 2014; Moore, 2006; Rong et al., 2015). Furthermore, business ecosystems have become a critical topic for strategy as these environments shape essential decisions about where and how firms should compete to achieve competitive advantages (Clarysse et al., 2014; Hanelt et al., 2021).

In multiple studies, business ecosystems are characterized by networks, interdependencies, partnerships, and value co-creation, promoting shared business processes, facilitating trust-building among contributors, and providing infrastructures for collaboration (e.g., Adner & Kapoor, 2010; Autio & Thomas, 2020; Graça & Camarinha-Matos, 2017; Hanelt et al., 2021; Hoch & Brad, 2021; Kapoor, 2018; Rong et al., 2015; Subramaniam et al., 2019). Companies that operate in business ecosystems instead of more traditional hierarchical integrated supply

chains increasingly adopt new organizational structures to promote business collaboration for resilience and agility in networks of strategic partnerships (Adner & Kapoor, 2010; Clarysse et al., 2014; Graça & Camarinha-Matos, 2017; Hanelt et al., 2021; Immonen et al., 2014; Kapoor, 2018; Rong et al., 2015). Rather than collaborating only with directly linked partners in traditional supply chains, business ecosystems support companies in implementing broader cross-industry collaboration among interdependent organizations (Adner & Kapoor, 2010; Rong et al., 2015). Kapoor (2018) further raises the role of complementarities between actors in business ecosystems, as the functions performed by various companies are connected within the system and affect the value created for end users. Hence, such complementarities and interdependencies between members contribute to the value propositions in business ecosystems (Kapoor, 2018).

Since scholars started considering the business ecosystem concept, the research has developed to include other forms of ecosystems, such as innovation ecosystems, entrepreneurial ecosystems, knowledge ecosystems, and digital ecosystems (Gupta et al., 2019; Scaringella & Radziwon, 2018; Tsujimoto et al., 2018). More recently, along with the digital transformation and diffusion of technologies through industries and society, digital business ecosystems (DBEs) are becoming increasingly relevant across sectors (Hanelt et al., 2021; Senyo et al., 2019). DBE represents a subtype of the business ecosystem where digital technology plays a dominant role in a collaborative environment consisting of different actors that co-create value, enhancing mechanisms of self-organization through digital infrastructure (Lenkenhoff et al., 2018; Scaringella & Radziwon, 2018; Senyo et al., 2019). Hence, DBEs are a combination of digital and business ecosystems, where digital ecosystems refer to a virtual environment of hardware, software applications, and digital processes that operate as technology infrastructure to connect services through shared digital platforms (Senyo et al., 2019). DBEs have gained increasing attention by facilitating open and flexible collaboration and competition by leveraging external resources, such as technology and specialized services, to respond to growing customer needs (Senyo et al., 2019). Furthermore, value in DBEs is created through resources, efforts, and interactions between ecosystem participants, taking financial or non-financial forms resulting from low-cost, high-quality services and more efficient processes (Senyo et al., 2019). As in any business ecosystem, the value created in DBEs is presumed to be greater than what a single firm could achieve, leading to synergies between ecosystem participants to generate strategic benefits through value co-creation and interdependence for a stronger value proposition (Senyo et al., 2019).

2.1.1 Opportunities of Business Ecosystem Participation

By strategically participating in business ecosystems, companies can achieve multiple advantages (e.g., Clarysse et al.; Fuller et al., 2019; Immonen et al., 2014; Jacobides et al., 2018; Lenkenhoff et al., 2018; Moore, 2006; Zahra & Nambisan, 2012). Companies can access critical resources, including financial capital, and overcome knowledge gaps through information about market conditions (Clarysse et al., 2014). Furthermore, business ecosystems can enable companies to build meaningful relationships with alliance partners while offering the opportunity to collaborate and compete with ecosystem members simultaneously through innovation (Zahra & Nambisan, 2012). For instance, the loosely coupled layers of digital objects in DBEs can enable participating companies to collaborate on technical aspects, such

as digital services, while competing on other layers, such as customer-oriented solutions (Lenkenhoff et al., 2018). These advantages promote opportunities to navigate the changing dynamics of markets and competitive environments (Clarysse et al., 2014; Zahra & Nambisan, 2012).

Business ecosystems can support interrelated and autonomous companies in activity coordination (Jacobides et al., 2018). For instance, a modular architecture can enable independent system parts to be developed by different actors with limited coordination (Jacobides et al., 2018). This modularization structure has contributed to the increasing prevalence of business ecosystems across various sectors, including financial services (Jacobides et al., 2018). Instead of simultaneously developing within multiple fields or being required to make high investments in uncertain projects, companies can focus on a narrower set of outcomes while gaining commitment for collaboration from other ecosystem members (Moore, 2006). Furthermore, business ecosystems can enable companies to manage the trade-off between commitment and flexibility by combining capacities without being required to commit to each specific combination in-house (Fuller et al., 2019). For instance, companies that operate in DBEs can commit to building a platform while remaining flexible about what services the platform will deliver by using third parties to develop those services (Fuller et al., 2019). Hence, business ecosystems can enable companies to explore different business opportunities across the system in parallel, which one traditional organization might not have the time, resources, or risk tolerance to perform in-house (Fuller et al., 2019). Such coordination of business ecosystems could enable companies to accept larger projects and invest their resources in more rapid internal innovation instead of managing interdependencies and uncertainties (Immonen et al., 2014; Moore, 2006). Furthermore, since business ecosystem members can integrate with other members through relatively simple interfaces, Moore (2006) points out that companies could focus on managing the issues within their specific domains while partially ignoring the problems in others.

According to Moore (2006), members of business ecosystems share the cost of the whole community, creating benefits for participating companies in new market creation. For instance, none of the other business ecosystem members could have afforded to establish the mainstream personal computer market without the expenditures covered by IBM's multi-dollar ad campaign where customers could try the new machines in IBM computer stores (Moore, 2006). Companies such as Intel, Microsoft, and other less-established actors benefited from this market creation, and ecosystem members could gather and maintain a shared vision of the market future that they would all contribute to creating (Moore, 2006). Figure 2.1 presents a summary of the opportunities for business ecosystem participation.

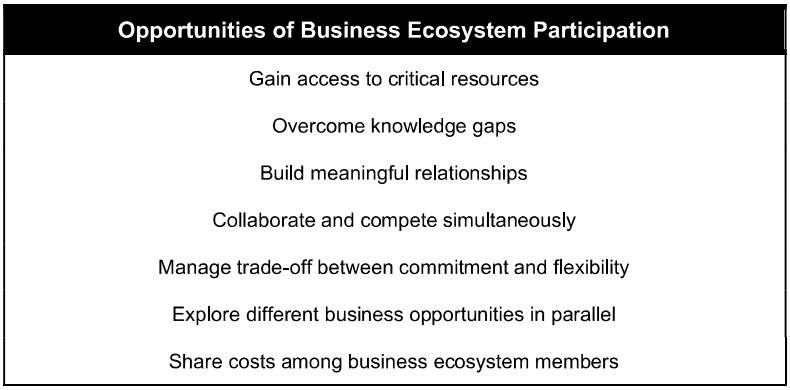

Figure 2-1: Opportunities of business ecosystem participation.

2.1.2 Challenges of Business Ecosystem Participation

Despite the opportunities and potential for value co-creation in business ecosystems, studies indicate that these environments also create multiple challenges for participating companies (e.g., Adner & Kapoor, 2010; Baldwin, 2012; Kapoor, 2018; Kim et al., 2010; Koenig, 2013; Lenkenhoff et al., 2018; Moore, 2006; Ramezani & Camarinha-Matos, 2020; Rong et al., 2015; Tsujimoto et al., 2018; Zahra & Nambisan, 2012). Hence, managers should not take the success and profitability of business ecosystems for granted (Baldwin, 2012). Competitive dynamics and cooperation processes often shift over time as business ecosystems shape and transform (Rong et al., 2015; Zahra & Nambisan, 2012). According to Zahra and Nambisan (2012), these changing dynamics create managerial and entrepreneurial challenges for participating firms to set and follow strategies since several situations require deliberate moves while others call for improvisation. Hence, participation in business ecosystems requires constant adaptation toward unpredictable and complex system behavior, preparation for the unknown future, and refinement of strategic actions, adding complexity to decision-making processes (Ramezani & Camarinha-Matos, 2020; Zahra & Nambisan, 2012).

According to Rong et al. (2015), companies operating in business ecosystems share a common fate as they depend on each other to reach common strategic objectives. Furthermore, such interdependence connects the offers various companies create for shared value-creation (Kapoor, 2018; Kim et al., 2010). Hence, participation in business ecosystems could increase the dependency on third parties through outsourcing and global partnerships for collaboration and value co-creation (Ramezani & Camarinha-Matos, 2020). Despite the possibilities of achieving more agile and efficient business operations, such cooperation could create vulnerability and new risks as companies open their borders and the dependency on third parties, such as suppliers, increases (Ramezani & Camarinha-Matos, 2020). Furthermore, a system built of multiple components could increase the risks of bottlenecks, affecting business ecosystem performance (Kapoor, 2018). According to Kapoor (2018), bottlenecks could lie upstream or downstream within input-output flows and change over time, limiting growth and demand by affecting the business ecosystem value proposition through cost, performance, or scarcity constraints. Additionally, complement innovation challenges could create complement availability delays as companies struggle with overcoming their internal technology problems, limiting the value creation in business ecosystems (Adner & Kapoor, 2010).

Various companies define their own strategies concerning ecosystem structure, roles, and risks, which could create contradiction rather than consistency (Adner, 2017). According to Tsujimoto et al. (2018), each company has different purposes and decision-making standards, causing risks of unintended business ecosystem outputs. Inconsistent strategies between members might not be recognized within a given period, leading to non-convergent and misleading actions for investments and the pursuit of value propositions, as companies have wrong beliefs about the end goals and motivations of other members (Adner, 2017). Furthermore, companies might struggle with designing their internal organizations for effective management of interdependencies with other business ecosystem members (Kapoor, 2018).

The requirements of collaboration and alignment in business ecosystems could create challenges if firms fail to address the importance of interfirm relationships and coordination (Koenig, 2013; Moore, 2006; Ramezani & Camarinha-Matos, 2020). In practice, Moore (2006) explains that companies often struggle with cooperation as the immediate and pressing work of managing the internal business distracts members away from community concerns. According to Lenkenhoff et al. (2018), alignment challenges could arise since participating firms often have different organizational structures and procedures for responsibilities, autonomy, and decision-making, along with varying cultures and communication standards. Additionally, although business ecosystem members could benefit from shared costs, financing challenges could arise as companies have different internal economics and varying funding needs (Moore, 2006). Immonen et al. (2014) underline how cooperation could suffer if the profits generated through a business ecosystem are not fairly distributed among members.

Companies could suffer from challenges in managing the interoperability, interconnectivity, and competing interests that participation in business ecosystems depends on for success (Lenkenhoff et al., 2018). For instance, technological challenges in DBEs, including underdeveloped digital interfaces and rules for data exchange among ecosystem members, could create barriers to achieving coordinated memberships (Lenkenhoff et al., 2018). Hence, firms could struggle to achieve sufficient compatibility with digital architectures, infrastructures, and platforms (Lenkenhoff et al., 2018). Figure 2.2 presents a summary of the different challenges of business ecosystem participation.

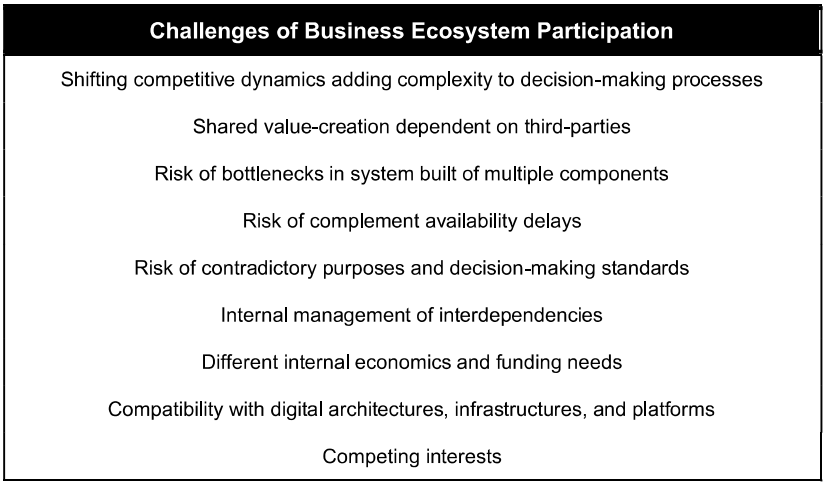

Figure 2-2: Challenges of business ecosystem participation.

2.1.3 Managing Business Ecosystem Challenges

Multiple studies indicate that alignment and agreement among participating members are critical to managing challenges and achieving successful business ecosystem outcomes (e.g., Adner, 2017; Immonen et al., 2014; Koenig, 2013; Lenkenhoff et al., 2018; Moore, 2006). Successful collaboration in business ecosystems requires agreement between members about shared project development and alignment on visions for synergistic value-adding and mutually beneficial processes (Koenig, 2013; Lenkenhoff et al., 2018; Moore, 2006). Koenig (2013) points out that the creation and maintenance of agreements is necessary for achieving successful collaboration in the long term. Furthermore, decision-making process alignment is crucial for building trust among members (Lenkenhoff et al., 2018). Vision alignment could support mutually beneficial and synergistic investments, reduce the challenges of cooperation, and increase the focus on co-evolution through community concerns rather than internal business issues (Adner, 2017; Moore, 2006). Companies could set up protocols and establish interfaces for individual contributions, roles, and services to support these alignments (Immonen et al., 2014; Moore, 2006). For instance, the responsibilities and division of work between members should be clearly defined for each task (Immonen et al., 2014). According to Lenkenhoff et al. (2018), individual companies should be able to contribute with collaborative and creative attitudes, competencies, and engagement. At the same time, value co-creation and co-evolution on a collective level require clear role definitions between members concerning subordination and interdependence (Immonen et al., 2014; Lenkenhoff et al., 2018).

Alignment gaps could arise from members' challenges in undertaking new activities for ecosystem contribution, lacking incentives and priorities to perform these activities, or varying expectations regarding ecosystem structures and roles, such as positions and responsibilities (Adner, 2017). Hence, Adner (2017) argues that a successful business ecosystem strategy must explicitly assess and proactively manage these risks. According to Jacobides et al. (2018), the success of a business ecosystem depends on its rules of engagement, standards, and interfaces. Standards could include requirements that participants agree to a minimal set of rules or more strictly controlled membership by a committee or ecosystem hub (Jacobides et al., 2018). Furthermore, Ramezani and Camarinha-Matos (2020) underline that participating companies must be willing to interact and share both their profits and risks. To address the challenges related to financing and profit distribution, cost- and profit-sharing arrangements could be implemented to include the ratio of work performed by each member, creating fair mechanisms and enabling a win-win situation for participating companies (Immonen et al., 2014).

Studies highlight that business ecosystems must create value for end consumers to generate successful outcomes (e.g., Moore, 2006; Zahra & Nambisan, 2012). Hence, Moore (2006) explains how ecosystem members must sustain transparency and close dialogues with customers to assess their needs and willingness to pay for products and services. Rather than outsmarting the competition, Zahra and Nambisan (2020) argue that companies should adopt novel strategies and approaches to creating customer value considering the whole business ecosystem. Figure 2.3 presents a summary of how companies could manage business ecosystem challenges, related examples, and their impact on the business ecosystem.

Management Area	Examples	Impact
Alignment and Agreement	Agreement on shared project development Visions alignment Decision-making process alignment	Successful long-term collaboration Trust and balanced exchange relationships Synergistic value-adding and mutually beneficial processes Clearly defined responsibilities and division of work Focus on co-evolution rather than internal business issues
Sharing of Both Profits and Risks	Address financing and profit distribution among members	Fair mechanisms for cost- and profit sharing Win-win situation for participating companies
Focus on Customer Value	Sustain transparency and close dialogues with customers	Successful business ecosystem outcomes Customer value-creation considering the whole business ecosystem

Figure 2-3: Summary of how companies could manage business ecosystem challenges, related examples, and their impact on the business ecosystem.

2.2 Payment Industry

Among other sectors, business ecosystems have increasingly emerged in the payment industry (Panetta et al., 2023; Passi, 2018). Driven partly by technological advancements in the banking industry and the arrival of electronic commerce (e-commerce), multiple studies indicate that the global payment industry has undergone a rapid transformation during the past decades (e.g., Bezovski, 2016; Furst et al., 1998; Gupta, 2013; Khan et al., 2017; Liu et al., 2015; Nelms et al., 2018; Passi, 2018; Sullivan, 2010). The emergence of fintech has driven technological advances, such as information and communication technology developments, and changed the dynamics of the banking structure (Furst et al., 1998; Gomber et al., 2017; Liu et al., 2015). At the same time, the arrival of e-commerce has introduced new ways for businesses and consumers to do trade business (Bezovski, 2016). During the past two decades, the global e-commerce market has significantly grown while providing benefits for companies and customers (Bezovski, 2016; Yao et al., 2018). Multiple studies suggest that technological advances and the growth of e-commerce have contributed to a shift in the payment industry toward diversified and electronic online payments (e.g., Bezovski, 2016; Furst et al., 1998; Khan et al., 2017; Nelms et al., 2018; Yao et al., 2018). These developments in the payment industry have contributed to the emergence of new business ecosystems and a shift from competition between actors to collaboration (Passi, 2018).

2.2.1 Financial Technology

The digital disruption of the payment industry has been driven by the emergence of fintech (Gomber et al., 2017). Fintech has emerged by enabling technological advances, such as infrastructure availability and affordability through the internet and mobile technology, and technology applications, including platforms and big data analysis (Leong et al., 2017). Hence, fintech companies use financial technology to challenge traditional business models, changing how financial services are offered and enhancing customer centricity (Gomber et al., 2017; Milian et al., 2019; Romānova et al., 2018). The emergence of fintech has changed the business landscape of the payment industry, modernizing payment infrastructures and pushing for new innovative financial services (Gomber et al., 2017; Romānova et al., 2018; Romānova &

Kudinska, 2016). Hence, the rapid emergence of fintech has impacted financial institutions, merchants, regulators, and customers across multiple sectors (Kou et al., 2021; Leong et al., 2017; Milian et al., 2019).

Fintech is considered one of the most critical innovations in the payment industry, contributing to higher-quality financial services, decreased costs, and improved customer satisfaction (Kou et al., 2021). Furthermore, innovative financial products and services offer enhanced convenience for consumers while cost-effectively increasing efficiency (Leong et al., 2017). Gomber et al. (2017) underline that one of the main advantages of fintech is the potential to decrease customer acquisition costs by generating targeted consumer recommendations by utilizing big data. For instance, fintech companies have partnered with external actors in the payment industry, such as credit card companies, investment firms, insurance providers, and banks, to build platforms and new services for improved customer acquisition (Gomber et al., 2017). Furthermore, fintech has allowed customers to provide third parties access to their financial data for enhanced customer experiences (Gomber et al., 2017). For instance, the fintech company PayPal has integrated APIs to connect its software applications with banks to access customer data and improve its payment service offerings (Gomber et al., 2017). Fintech has contributed to non-bank technology companies entering the payment market (Gomber et al., 2017; Liu et al., 2015). According to Liu et al. (2015), new actors, such as startups, technology firms, internet giants, and telecoms, have entered the market due to the high expected returns. Furthermore, fintech companies have focused on applications to reduce transaction costs for international payments, affecting market structures and how payment services are offered (Gomber et al., 2017).

Traditional banks and credit card companies possess critical advantages in the payment industry, such as reliable infrastructures for financial transactions, existing merchant networks, and consumers' trust (Gupta, 2013). However, despite these advantages, fintech poses critical threats to these companies as the entrance of technology firms into the payment industry has affected competition and market uncertainties (Lee & Shin, 2018; Liu et al., 2015; Passi, 2018; Romānova et al., 2018). Hence, traditional financial institutions increasingly develop strategies for competition, coexistence, and collaboration with fintech actors and integrate and invest in fintech to gain competitive advantages in the competitive dynamics of the payment industry (Gomber et al., 2017; Kou et al., 2021; Lee & Shin, 2018; Romānova & Kudinska, 2016). For instance, banks increasingly collaborate with fintech companies to develop novel capabilities for new technology, enhance organizational efficiency, and increase their market value (Gomber et al., 2017; Gupta, 2013; Kou et al., 2021).

Despite the opportunities of fintech in the payment industry, multiple studies indicate that fintech companies are encountering multiple risks and challenges (e.g., Leong et al., 2017; Liu et al., 2015; Passi, 2018; Romānova & Kudinska, 2016). According to Liu et al. (2015), new technologies in the payment industry create risks and uncertainties for companies, such as changing customer preferences, technological risks, and competition threats. Fintech companies face significant competition from incumbents and new market entrants that constantly transform their financial service offerings (Leong et al., 2017; Romānova & Kudinska, 2016). Hence, as in most industries with strong incentives for innovation, the competition between financial services providers is high (Khan et al., 2017; Passi, 2018). The

forces enabling reduced customer acquisition costs have also decreased the switching costs for consumers to move to competitors (Gomber et al., 2017). Furthermore, fintech companies face challenges in building a profound understanding of and achieving compliance with the regulatory and legal requirements in the payment industry (Gomber et al., 2017; Leong et al., 2017). Finally, the arrival of new technologies in the payment industry, their impact, and future development are hard to predict (Gomber et al., 2017; Liu et al., 2015). Hence, Gomber et al. (2017) argue that fintech companies increasingly need to focus on coordination, operational efficiency, and customer centricity to retain their customers. Passi (2018) further argues that fintech companies need to renew their distribution channels to make payments easier, faster, and more accessible, while focusing on the security of transactions.

2.2.2 Online Payments

Along with the emergence of fintech and the growth of e-commerce, online payments have significantly increased (Bezovski, 2016; Furst et al., 1998; Khan et al., 2017; Nelms et al., 2018; Yao et al., 2018). Online payment options can take various forms (Bezovski, 2016; Iman, 2018; Khan et al., 2017; Nelms et al., 2018). Credit and debit cards have dominated most transaction markets for online purchases (Bezovski, 2016; Khan et al., 2017), which Sullivan (2010) explains has been due to the convenience perceived by customers and their wide acceptance rate among merchants. However, along with the advancement of technology, other online payment options have developed during the past years, such as digital and mobile wallets, electronic cash, smart cards, contactless payment methods, and mobile payments (Bezovski, 2016). Mobile payments have disrupted the global payment industry by enabling consumers to make payments through mobile devices (Bezovski, 2016; Gupta, 2013; Lee & Shin, 2018). Mobile payments depend on payment credential tokenization, which reduces the risk of data breaches and enhances consumer fraud protection while enabling improved risk management standards (Liu et al., 2015). According to Khan et al. (2017), the security and convenience offered by mobile payment options outperform debit and credit card payments in these aspects, which has contributed to the global growth of mobile payments.

Studies indicate that online payments and mobile technology have significantly impacted the global payment industry (e.g., Bezovski, 2016; Gupta, 2013; Iman, 2018; Khan et al., 2017; Ondrus & Pigneur, 2009). Customers can benefit from multiple advantages when using a mobile device for online payments, such as enhanced convenience through a broad variety of purchasing possibilities, location-free access, and a simple alternative to physical payments (Bezovski, 2016; Ondrus & Pigneur, 2009). As a result of the improved customer convenience and efficiency of transactions, online payment offerings could improve long-term customer retention (Gomber et al., 2017). Mobile payments offer opportunities for banks to increase the convenience of their financial services for existing customers while reaching customers in emerging markets with mobile devices who have not yet adopted bank accounts (Gupta, 2013). Hence, banks have increasingly invested in technology and mobile security by developing smartphone applications and new convenient features, promoting mobile banking adoption among consumers (Gupta, 2013). Besides traditional banks and credit card companies, new players have emerged in the mobile payment market (Gupta, 2013; Yao et al., 2018). For instance, in 1998, PayPal pioneered in the US with its online payment services supported on mobile devices, guaranteeing transaction security in the e-commerce environment for

consumers and businesses (Yao et al., 2018). A few years later, in 2004, Alibaba Group introduced Alipay – China's most commonly used online payment intermediary presently (Yao et al., 2018).

Business ecosystems in the mobile payment market involve large value chains spanning multiple organizations from diverse business industries, including mobile network operators, payment and banking services, software developers, and semiconductor producers (Coskun et al., 2013). Companies in the mobile payments sector have realized the potential in these business ecosystems due to the potential for business opportunities and a shared agreement that no single firm can provide these services to end users (Coskun et al., 2013). However, the adoption of mobile payment services has been slower than expected (Coskun et al., 2013; Guo & Bouwman, 2016). According to Coskun et al. (2013), the reason for the slow adoption rate has been that the ecosystem structure and its value chain have not been clearly defined since participating companies have not agreed on a common understanding and shared vision for the underlying technology, leading to the lack of a mutually beneficial business model. The high number of members across various sectors further makes the business ecosystem of mobile payments complex (Liu et al., 2015). Coskun et al. (2013) highlight that the high potential for shared profits in the business ecosystem causes misalignment between members regarding suitable business models. Additionally, members of these ecosystems are often influential in their respective industries, making them used to other parties following their needs (Coskun et al., 2013).

Coskun et al. (2013) and Guo and Bouwman (2016) raise interoperability, compatibility, and standardization of the underlying mobile technology, along with ecosystem cooperation, as critical to achieve successful business ecosystem outcomes. According to Liu et al. (2015), a company's ability and willingness to participate in cross-industry collaboration for payment innovation depends on its access to resources, individual perception of the risks of future technological changes and market uncertainties, and ability to obtain and process market information. Mobile payment platform providers, such as Apple Pay, Google Wallet, and Softcard, cooperate in cross-industry alliances to implement shared operational, technology, and process standards to foster innovations in the ecosystem (Liu et al., 2015). According to Liu et al. (2015), Apple managed to enhance the consumer adoption of Apple Pay and achieve support from merchants and banks by cooperating with VISA, Mastercard, and American Express for its business infrastructure.

Despite the advantages of online payments compared to conventional payment methods, such as enhanced convenience and higher security standards, online financial services providers face several challenges (Gomber et al., 2017; Khan et al., 2017). For instance, Khan et al. (2017) argue that the effective execution of online payments requires clear structures for legal and regulatory standards. The lack of such structures could make it difficult for online financial services providers to provide their services globally effectively (Khan et al., 2017). Furthermore, for innovations to succeed in the payment market, Gomber et al. (2017) argue that consumers must be confident that their privacy and security are ensured (Khan et al., 2017). According to Khan et al. (2017), online financial services providers should ensure integrity, confidentiality, and availability to gain trust and acceptance from consumers. Finally, Khan et al. (2017) explain that payment systems supporting online payments must be sufficiently secure

and compatible with traditional payment infrastructures to ensure operational efficiency. According to Khan et al. (2017), online financial services providers should consider interoperability, universal standards, and flexible solutions when designing their payment offerings, along with the balance between security and usability to ensure customer value.

2.3 Financial Crime

Along with the growth of e-commerce, the emergence of fintech, and the increasing adoption of online payments, the global payment market faces several challenges (Bezovski, 2016; Khan et al., 2017; Sullivan, 2010). Despite the opportunities created by e-commerce for merchants and consumers, online payments for these transactions have increased financial crime risks, leading to new privacy and security concerns (Bezovski, 2016; Bolton & Hand, 2002; Hutchings & Holt, 2015; Khan et al., 2017). Fraud, identity theft, and the lack of security and consumer trust pose some of the main barriers to e-commerce (Bezovski, 2016; Yao et al., 2018). The development of fintech has driven significant volumes of digital transactions, increasing the challenges of efficiently managing risks related to financial crime (Giudici, 2018; Jullum et al., 2020).

2.3.1 Money Laundering and Fraud

Financial crime is defined as any non-violent crime resulting in a financial loss, including money laundering, fraud, and other illegal activities, such as using financial services to support criminal businesses (Hasham et al., 2019; International Monetary Fund, 2001). Money laundering can take place in different forms, such as “washing” of the money by eliminating any possible connection with previous criminal activities or carrying out other operations to hinder the identification of criminal roots of the goods (Faccia et al., 2020). Fraud is often approached as a loss problem and includes crimes such as credit scams, forgery, and insider threats, involving the abuse of financial services to commit theft (Bolton & Hand, 2002; Hasham et al., 2019; Ngai et al., 2011).

Historically, criminals have often exploited weaknesses in banks’ relatively straightforward controls for payment fraud to complete transactions unauthorized by the real account holder for financial advantages (Gupta et al., 2022; Sullivan, 2010). However, criminals are increasingly exploiting the security vulnerabilities of payment instruments to access unauthorized and sensitive payment data, resulting in extensive data breaches to develop more complex forms of payment fraud (Sen & Borle, 2015; Sullivan, 2010). As a result, payment security concerns and awareness of identity theft and fraud have increased (Bolton & Hand, 2002; Sullivan, 2010). In 2022, nearly $8.8 billion in financial consumer losses were reported to the US Federal Trade Commission (FTC) System due to fraud, indicating an increase of 30% since the year before (Consumer Sentinel Network, 2022). Furthermore, money laundering detection is increasingly challenging as money launderers use more sophisticated methods (Buehler, 2019). Although difficult to estimate, the UN Office on Drugs and Crime has reported annual money laundering amounts to be reaching 5% of global GDP, or up to $2 trillion (Mikkelsen et al., 2022). Despite new solutions to combat financial crime, the leverage and abuse of financial technologies by criminals continue to grow (Nikkel, 2020).

Financial services providers and merchants use information-intensive systems for transaction approval to prevent fraud (Sullivan, 2010). The possibilities of making more accurate and automated approval decisions increase as more information is taken into account, incentivizing continuous expansion of information collection while raising the reliance on data (Sullivan, 2010). However, Sullivan (2010) explains how the incentives for criminals to collect the same data for committing payment fraud grow simultaneously. These increasing incentives for both sides to collect more data lead to an escalating cycle as financial services providers and merchants use more resources to protect their data, and criminals use more resources to compromise the same data (Sullivan, 2010).

Financial crime increases various risks for companies in the payment industry, such as operational risk, involving the risk of loss caused by inadequate or failed processes, systems, people, or external events (Chapelle, 2019; Girling, 2022; Mikkelsen et al., 2022). These risks create challenges involving financial loss, regulatory non-compliance, reputational damage, customer detriment, and decreased trust of clients (Bolton & Hand, 2002; Buehler, 2019; Chapelle, 2019; Mikkelsen et al., 2022). According to Gomber et al. (2017), the high expenses associated with missing fraudulent transactions have created incentives for financial companies to invest in and develop refined machine learning algorithms for fraud detection. Mobile payments have enabled companies to leverage and consolidate real-time location data for financial crime detection through such sophisticated algorithms (Gomber et al., 2017). However, the data consolidation simultaneously makes companies more exposed to data breach risks if hackers manage to gain access to all the financial customer data (Gomber et al., 2017).

2.3.2 Increasing Regulation

As a response to the increasing concerns about fighting financial crime in the payment industry, regulators are taking actions to counter such criminal activities (Mikkelsen et al., 2022; Gomber et al., 2017; Grasshoff et al., 2021; J. P. Morgan, 2021; Passi, 2018; Romānova et al., 2018). According to Gomber et al. (2017), the emergence of fintech has increased the transaction speed, raising the need for public policy and governmental regulation to combat criminal transactions. In 2016, the European Union adopted the Revised Payment Services Directive (PSD2), which aimed at increasing the efficiency of the European payment market, enhancing consumer protections, and creating a safer environment throughout the online payments landscape (European Central Bank, 2018; Passi, 2018). According to Deloitte (2018) and Mikkelsen et al. (2022), this directive is likely to be reviewed soon with an enhanced focus on financial crime. Furthermore, the European Commission (EC) has announced plans to launch a new EU authority to counter financial crimes, such as money laundering, and enhance the existing EU framework on such criminal activities (Mikkelsen et al., 2022).

2.3.3 Managing Financial Crime Risks

Studies indicate a need for high-security standards and effective countermeasures to prevent the exploitation of security vulnerabilities to fraud (Bezovski, 2016; Sullivan, 2010). Some examples of how financial companies can manage financial crime risks include establishing and following a firm-wide risk appetite, performing KYC reviews of customers, and implementing collaborative measures to respond to the complexity and damaging consequences of these risks.

2.3.3.1 Risk Appetite

Regulators are increasingly pushing for actors in the payment industry to implement robust frameworks and better articulate their risk appetite to support effective risk management (Girling, 2022; Gontarek, 2016; Rittenberg & Martens, 2012). For instance, the Basel Committee on Banking Supervision (BCBS) has presented standards for how financial institutions and their regulators can manage operational risk while addressing the importance of defining risk appetite to support these frameworks (Girling, 2022; Gontarek & Bender, 2019). In 2015, BCBS provided the following definition of risk appetite: *"The aggregate level and types of risk a bank is willing to assume, decided in advance and within its risk capacity, to achieve its strategic objectives and business plan."* (Girling, 2022).

Gontarek and Bender (2019) suggest that establishing a firm-wide risk appetite impacts financial companies' activities and ideally considers strategy, stakeholders' interests, risk capacity, business conditions, and the overall competitive environment. Girling (2022) further explains how operational risk requires fintech companies to demonstrate effective measurement and management through quantitative and qualitative approaches for successful business plan execution. When managing financial crime risks, companies should decide which risks are within their risk appetite and that they are willing to accept versus are outside their risk appetite (Mikkelsen et al., 2022). According to Mikkelsen et al. (2022), these decisions become critical as, for instance, certain KYC issues impact essential parts of the business model, such as the customer experience, including onboarding and transactions. Furthermore, Fritz-Morgenthal et al. (2018) highlight that companies must have clear plans for how to respond if risks exceed acceptable levels according to the risk appetite. To prepare for these situations, companies should identify possible negative scenarios and the strategies for mitigating these before a crisis occurs (Fritz-Morgenthal et al., 2018).

Studies suggest that companies should continuously update their risk appetite to reflect their objectives and understand the trade-offs involving higher or lower risk appetite levels as their business models change (Jain et al., 2020; Rittenberg & Martens, 2012). Furthermore, Jain et al. (2020) underline that the risk amount a company is willing to take must reflect its competitive landscape, shifting customer behaviors, digital capabilities, and global trends. For many risks, Jain et al. (2020) and Rittenberg and Martens (2012) note how companies need to apply a nuanced perspective built on objective facts as the lines for risks are not clear, while continuously updating these views as their environment, fact base, and business model change. Additionally, Rittenberg and Martens (2012) argue that risk appetite plays a critical role for companies in achieving their strategic objectives. Hence, managers should be responsible for determining the risk appetite following three steps, as illustrated in Figure 2.4 (Rittenberg & Martens, 2012).

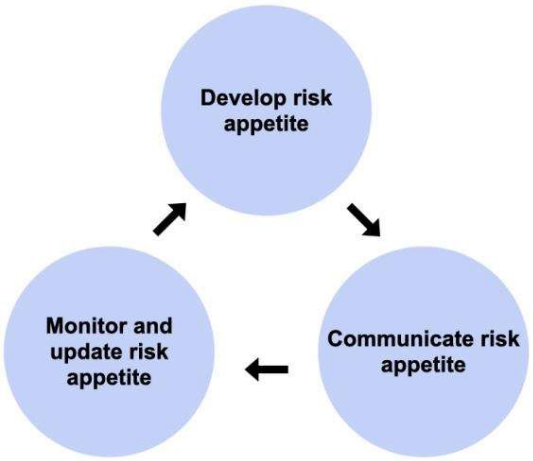

Figure 2-4: The steps managers should take when determining the risk appetite (Rittenberg & Martens, 2012).

2.3.3.2 Know Your Customer

Apart from establishing and following a firm-wide risk appetite, one way for financial companies to manage financial crime risks is through KYC reviews (Khan et al., 2017; Malhotra et al., 2022; Rajput, 2013). KYC regulations and guidelines have been implemented across financial markets to avoid the involvement of financial companies in financial crime activities (Gomber et al., 2017). Hence, KYC is a legal and regulatory requirement used by financial companies to verify new and existing customers' identities and to understand their risk and financial profiles before and after onboarding (Gomber et al., 2017; Malhotra et al., 2022; Taherdoost, 2023; Yadav & Chandak, 2019). According to Arner et al. (2019) and Rajput (2013), financial firms can ensure market integrity while guarding against money laundering and fraud by implementing KYC processes including account monitoring mechanisms. Furthermore, sound KYC policies and procedures could contribute to reducing other significant risks, including legal and reputational risks (Rajput, 2013). KYC typically includes three components: customer identification program (CIP), customer due diligence (CDD), and enhanced due diligence (EDD) (Chen, 2022).

Financial companies increasingly use streamlined processes to adhere to KYC regulations (Gomber et al., 2017). For instance, companies could simplify the data acquisition and verification processes for KYC by implementing application programming interfaces (APIs) that enable users to connect their bank accounts with third-party applications, enabling simplified customer identification and validation by using the data provided by the bank (Gomber et al., 2017). However, despite more streamlined solutions, multiple studies indicate that financial companies are encountering challenges related to KYC as these processes are becoming increasingly complex and incurring higher expenses (e.g., Berg et al., 2020; Gomber et al., 2017; Parra Moyano & Ross, 2017; Schlatt et al., 2022; Yadav & Chandak, 2019). In 2016, the average cost for financial companies to meet their KYC obligations was $60 million, while several companies had to spend up to $500 million on these processes (Yadav & Chandak, 2019). Companies that fail to fulfill the KYC requirements risk exposure to high fines (Chen, 2020; Elliot et al., 2022; Yadav & Chandak, 2019). For instance, in 2016, the New York State Department of Financial Services (DFS) levied a fine of $180 million against

Taiwan's Mega Bank due to insufficient compliance mechanisms (Chen, 2020). Furthermore, between 2009 and 2019, banks worldwide paid over $30 billion in penalties for failing to restrict financial crime activities (Buehler, 2019). According to Buehler (2019) and Chen (2020), the complexity of KYC arises due to difficulties in obtaining necessary customer data, such as identity and address information, while the data quality often is low. Additionally, Chen (2020) mentions how firms struggle to use relevant monitoring mechanisms for KYC as financial crime patterns differ between markets and businesses, and abnormal transactions are hard to identify, often allowing criminals to avoid detection. At the same time, customers often experience poor KYC experiences as they must undergo the same process for each financial institution with which they intend to work (Schlatt et al., 2022; Yadav & Chandak, 2019). Apart from collecting and storing sensitive consumer data, financial companies struggle with satisfying their customers' privacy expectations (Gomber et al., 2017).

2.3.3.3 Collaborative Strategy

Financial companies are increasingly considering solutions to combat financial crime through a collaborative strategy involving ecosystems and partnerships to respond to the complexity and damaging consequences of operational risk (Scott et al., 2020; Van Rooijen et al., 2021). For instance, financial companies increasingly use technology-based outsourcing to cut costs and improve the efficiency of operational activities as a response to the challenges of fulfilling regulatory requirements (Gozman & Willcocks, 2019). Banks have increasingly partnered with fintech companies for improved KYC capabilities and fraud detection (Gomber et al., 2017). Multiple countries are further pursuing the collection and publication of fraud statistics as an initiative to guide the payment industry in its efforts to counterfeit financial crime activities (Sullivan, 2010).

Multiple initiatives have been launched across card issuers to increase the protection of sensitive data and counterfeit payment fraud (Khan et al., 2017; Sullivan, 2010). In 2004, Visa, Mastercard, and other card companies cooperated to implement the Payment Card Industry Data Security Standard (PCI DSS) (Sullivan, 2010). PCI DSS aimed at setting a common industry standard to help businesses and payment processors protect sensitive data by establishing secure networks, data encryption, robust access controls, and security policies (Sullivan, 2010). Furthermore, the card schemes Europay, Mastercard, and Visa (EMV) have implemented the EMV standard for payment cards, which American Express, Discover, and JCB also have accepted to combat fraud (Sullivan, 2010). Despite multiple advantages, card networks face barriers related to these initiatives (Sullivan, 2010). According to Sullivan (2010), the entire network security is compromised by different incentives of members to make individual efforts, increasing the dependency on the weakest links. In the same way that higher efforts of one member to improve the network security increase the benefits for other members, lower efforts by another member pose risks to the rest of the network (Sullivan, 2010). Hence, Sullivan (2010) argues that security efforts should be pursued through collaboration, while network standards should be cooperatively determined and flexible to manage conflicts of interest, satisfy various interests, and promote incentivization and compliance among all members. Additionally, the governance structure should include all actors and interests to prevent blocking of the network progress (Sullivan, 2010). Card networks have addressed the

risks of conflicts of interest by requiring a network membership to access its services, with potential penalty fees if any member fails to achieve compliance (Sullivan, 2010).

Similar to the initiatives launched by card networks, Bezovski (2016) suggests that diverse actors in the mobile payment market, such as mobile device manufacturers, payment service providers, and telecommunication companies, should cooperate to develop common platforms and ensure secure online payment environments. Sullivan (2010) indicates the need for enhanced coordination between various actors in the payment industry to improve the security of payment systems. Rather than investing in unneeded technology and developing separate systems for transaction monitoring and screening, financial companies and merchants could coordinate their efforts and identify solutions to achieve shared goals that benefit all members in the ecosystem (Sullivan, 2010).

Arner et al. (2019) and Steinert and Williams (2020) mention how financial companies could implement a shared KYC utility approach to address the risks of financial crime and regulatory pressure. By sharing information in a system of member institutions, companies could benefit from reduced risk, improved effectiveness of KYC processes, and enhanced operational efficiency while improving the customer experience and decreasing costs (Arner et al., 2019; Karadag et al., 2022; Schlatt et al., 2022; Steinert & Williams, 2020). Such KYC utilities could take different forms, such as collecting and sharing KYC data among utility members to improve and streamline onboarding processes and consolidating transaction-level data to enable refined transaction monitoring and screening (Steinert & Williams, 2020). They could also involve fully outsourced solutions to improve the efficiency and operations of KYC through non-bank third parties, such as technology or data vendors (Steinert & Williams, 2020). However, according to Steinert and Williams (2020), such outsourced solutions could form conflicting incentives between vendors and participating firms, as vendors might focus on capturing revenue from their products and services rather than creating value for the financial companies.

3. Methodology

This chapter presents the research design of the study, the methods applied for data collection and analysis, the research quality, and ethical considerations. A single-case study was performed to illustrate the topics that fintech companies need to consider when partnering with third-party actors for payment product distribution. The data collection relied on qualitative research through semi-structured interviews at the case company. Furthermore, a thematic analysis was conducted to analyze the data obtained during interviews. The trustworthiness of the study was evaluated by considering its credibility, transferability, dependability, and confirmability. Finally, ethical issues concerning potential harm to research participants, a lack of informed consent, an invasion of privacy, and deception were considered.

3.1 Research Design

This study has followed the research design of a case study. A case study can be an appropriate research method to use when the research questions intend to answer "how" and "why" questions and when the project focuses on contemporary events (Easton, 2010; Yin, 2009). Hence, since the research questions of this study were intended to answer how risks related to financial crime affect fintech companies, and how these could be managed, the case study was considered a suitable research design. Furthermore, case studies focus on the complexity and specific nature of a particular case, such as a single organization, and concentrate on creating an understanding of the dynamics present within this setting (Bryman & Bell, 2011; Eisenhardt, 1989). Therefore, it was considered appropriate to select a specific case company to study the issues and answer the research questions.

According to Stake (1995), researchers should select cases based on the potential for learning opportunities, where the expected learning is the greatest. Hence, the potential for learning opportunities related to the purpose and research questions of this study was considered when selecting a suitable case company. Furthermore, using a single-case study may be appropriate when the case is representative for an industry or when there is an opportunity to observe and analyze a problem previously inaccessible to social science inquiry (Yin, 2009). Therefore, the case company was further selected to represent situations that similar companies encounter and that have previously not been sufficiently studied.

3.1.1 Case Company

The case company for this study is a Swedish fintech company and online financial services provider that partners with third-party payment facilitators for payment product distribution. Through the partnerships with third-party payment facilitators, the case company seeks to acquire a broader network of merchants to achieve further growth while limiting direct financial loss exposure and decreasing operational costs by outsourcing various activities. However, due to the increased dependency on third-party payment facilitators, the case company needs to address several considerations, including risks related to financial crime.

The case company was suitable for this study to illustrate the topics that fintech companies need to consider when seeking to distribute their payment products through collaboration with third-party actors. By studying the case company and understanding the effects of financial crime risks associated with a distribution strategy through third parties, there was an opportunity to contribute to the research by identifying how fintech companies can collaborate with third-party actors in business ecosystems for payment product distribution considering these risks. Furthermore, by understanding how the case company could manage its partnerships considering financial crime risks, there was an opportunity to provide more general guidelines for how similar companies could manage various risks related to financial crime associated with a distribution strategy through third parties.

3.1.2 Study Context

This section presents the context in which the case company is situated. First, market aspects are presented, providing context on why similar actors in the payment industry collaborate with third-party payment facilitators for payment product distribution. Second, since the study will explore how the case company could manage risks related to financial crime when collaborating with third-party actors, context is provided on how similar actors control the risk exposure created by their partnerships through fraud monitoring programs.

3.1.2.1 Market Aspects

Following the increasing demand for online payments and changing customer preferences, the European Central Bank (2022) has reported that merchants accept an increasingly wide range of online payment options to cater to a greater variety of customers. In the "2022 Commerce and Payment Trends Report" by Global Payments (2022), 38% of surveyed merchants expanded their online payment options in 2021. During the following year, 53% of merchants expected to increase their number of online payment options (Global Payments, 2022). The European Central Bank (2022) found that one of the main barriers perceived by merchants to integrating new payment methods is the effort and time required for integration. Hence, merchants value the capacity to integrate multiple payment solutions into existing infrastructure through a single payment facilitator (European Central Bank, 2022; Global Payments, 2022; J.P. Morgan, 2021). By getting one set of APIs and one integration into the underlying technology, merchants can simplify the integration of a package of payment options by using one single provider (J. P. Morgan, 2021).

Multiple actors in the payment industry partner with third-party payment facilitators for payment product distribution, similar to the case company. For instance, credit card brands, such as Visa, Mastercard, and American Express, collaborate with multiple payment facilitators globally to support the integration of their payment methods for merchants and enable consumers to pay online using their card brands (Visa, 2018; Mastercard, n.d; American Express, 2023). Similarly, Apple, Google, and Alipay partner with payment facilitators to enable consumers to pay with a saved card or stored balance through their digital wallets when shopping online (Apple, n.d.; Stripe, n.d.).

3.1.2.2 Fraud Monitoring Programs

Fraud monitoring programs provide one example of how payment card networks control that the merchants they partner with fulfill financial regulations to limit their risk exposure (J. P. Morgan, 2022a; J. P. Morgan, 2022b). For instance, Visa and Mastercard have implemented fraud monitoring programs to reduce e-commerce fraud and increase the security of their payment ecosystems by controlling that merchants do not exceed certain financial crime-related transaction volumes (checkout.com, 2023; J. P. Morgan, 2022a; J. P. Morgan, 2022b). Merchants that exceed certain fraud volumes compared to their sales volumes are placed in the fraud monitoring program and must create remediation plans, outlining actions to restore compliance and including dates and milestones for all corrective actions (J. P. Morgan, 2022a; J. P. Morgan, 2022b). Based on the exceeded thresholds, merchants are assessed different levels of fines or other adverse actions (J. P. Morgan, 2022a).

3.2 Data Collection and Analysis

The data collection for this study has relied on qualitative research through semi-structured interviews at the case company. For the data analysis, a framework proposed by Grodal et al. (2021) was applied to generate a structure for the categorization of data and enable the formulation of conclusions.

3.2.1 Interviews

Semi-structured interviews were conducted with employees at the case company with knowledge in the studied field. Advantages of the semi-structured interview format include the ability of interviewers to improvise follow-up questions depending on the relevance of participants' replies and the room for participants' individual verbal expressions (Bryman & Bell, 2011; Kallio et al., 2016). The interview questions were determined in advance and formulated using an interview guide that covered the main topics of the study, which is considered beneficial to enable structured discussions while exploring the research topic by collecting similar data from all participants (Kallio et al., 2016). The interviews intended to create an understanding of how the case company is affected by risks related to financial crime when partnering with external actors for payment product distribution and scaling. For this purpose, interviews focused on topics related to payment product distribution through external payment facilitators and the areas that should be considered related to financial crime aspects. Furthermore, considerations for risk management from the case company's perspective were studied during interviews to identify potential measures to manage the risks related to financial crime when partnering with third-party actors in business ecosystems. This qualitative interviewing formed an inductive approach to the relationship between theory and research, which Bryman and Bell (2011) consider as beneficial in case studies as they are helpful in the generation of an intensive examination of the case.

In total, 11 interviews were conducted at the case company. Interviewees were selected based on their knowledge within the studied field and included employees with expertise in risk management, business development, and legal areas. Since the topics of this study mainly dealt with risks related to financial crime and how these could be managed, a majority of participants with risk management expertise were selected. All interviews were conducted online in a video

format due to the location of interviewees. The interviews were recorded with permission from participants and transcribed to enable deeper analysis of the material after conducting the interviews. In several cases, participants who had previously been interviewed were contacted again for follow-up questions as new information surfaced. Figure 3.1 presents the list of interviewees, their area of expertise, date, and duration of each interview.

Interviewee	Area of Expertise	Date	Duration (min)
A	Legal	2023-03-28	47
B	Risk Management	2023-03-28	58
C	Risk Management	2023-03-29	29
D	Risk Management	2023-03-29	41
E	Risk Management	2023-03-29	41
F	Risk Management	2023-03-30	41
G	Business Development	2023-03-30	29
H	Business Development	2023-04-05	36
I	Risk Management	2023-04-11	37
J	Risk Management	2023-04-12	46
K	Business Development	2023-04-12	29

Figure 3-1: List of interviewees, their area of expertise, date, and duration of each interview.

3.2.2 Data Analysis

A thematic analysis was conducted to analyze the data obtained during interviews. Data categories were generated by applying a general framework for qualitative analysis proposed by Grodal et al. (2021) to create the basis for new theory development. The framework included three stages: initial category generation, refinement of tentative categories, and stabilization of categories (Grodal et al., 2021). Figure 3.2 illustrates the framework and specific moves taken during each stage.

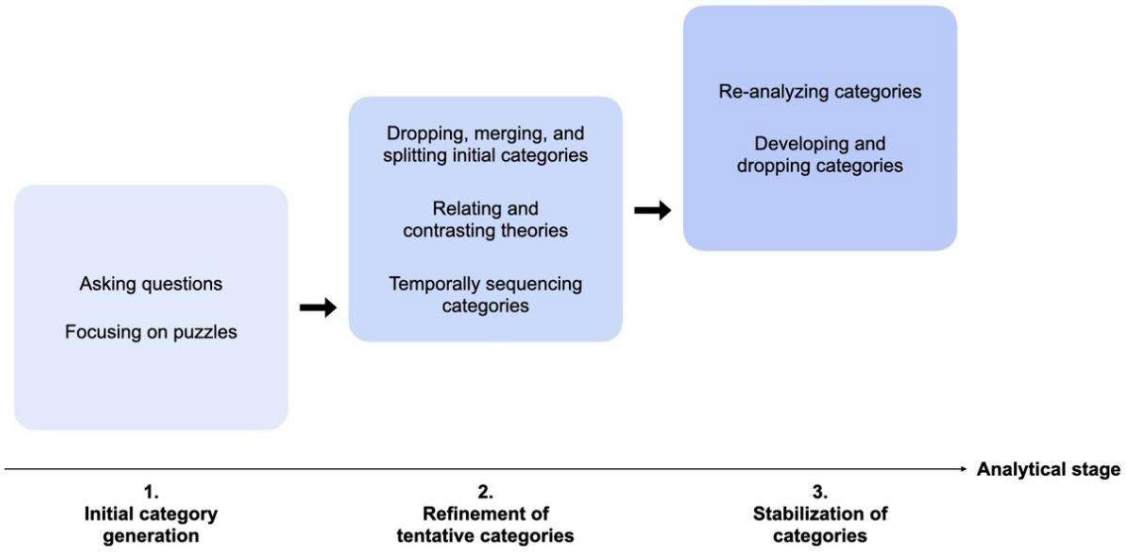

Figure 3-2: The applied framework proposed by Grodal et al. (2021) for data categorization and specific moves taken during each stage.

During the first stage, interviewees were asked predefined questions related to the research questions of the study and associated theories, focusing on three overarching categories: (1) opportunities of third-party payment product distribution, (2) considerations related to financial crime, and (3) risk management. Interviewees were asked questions such as "*From a financial crime perspective, what do you believe needs to be considered when distributing payment products through third-party payment facilitators?*" and "*How do you believe that these considerations could be managed?*". These initial questions allowed for proactivity by directing the qualitative analysis toward specific theories related to the study, which Grodal et al. (2021) explain increases the likelihood of theoretical significance. When developing initial data categories based on the answers to these questions, a focus was put on puzzles and identifying the data most relevant to answer the research questions of the study while partially ignoring less relevant data to support managing the complexity and high amount of data. As a result, initial data categorizations for each overarching category were identified.

Second, the initial data categories were analyzed and restructured according to the identified links between these. For instance, several categories were moved from the overarching data category "considerations related to financial crime" to "risk management" and vice versa since they were identified as more related to these categories. Some categories were split into separate categories to increase the clarity of the distinction between concepts, while other categories were merged into one due to their close relatedness. Categories were further sequentially structured along with the recognition of dynamic relationships. For instance, the various solutions for how considerations related to financial crime could be managed were categorized into different sequential stages of the partnerships with third-party payment facilitators, such as pre-onboarding, post-onboarding, and throughout the relationships. According to Grodal et al. (2021), these moves could help researchers differentiate between and map out links between categories functioning as mechanisms or concepts. Furthermore, it

allows for new perspectives on the interrelationships between mechanisms and concepts, creating a more exhaustive understanding of concepts (Grodal et al., 2021).

Third, during the final step of the analysis, the results generated from the interviews were reanalyzed and integrated with the information presented in the theoretical framework in Chapter 2. The obtained results were compared and contrasted with theories to identify supporting and opposing evidence to, finally, enable the formulation of conclusions. According to Grodal et al. (2021), these moves enable the stabilization of a categorization structure that supports hypotheses and advances theory.

3.3 Research Quality

The case company was considered a relevant case for this study to illustrate the topics related to financial crime risks that fintech companies need to consider when seeking to distribute their payment products through third-party actors in business ecosystems. According to Lee et al. (2007), the main strength of a case study is particularization rather than generalization. Hence, the goal of this study was to generate concepts of how financial crime risks can be managed by exploring the particular case and creating an understanding of the complexity related to the case company's distribution partnerships with third-party payment facilitators. However, Bryman and Bell (2011) raise issues of trustworthiness for assessing qualitative studies. To determine the trustworthiness of a study, Bryman and Bell (2011) point out credibility, transferability, dependability, and confirmability as equivalent criteria that should be considered.

3.3.1 Credibility

Achieving credibility in qualitative research involves ensuring good research practice and receiving respondent validation to confirm that the researcher has understood the studied issue correctly (Bryman & Bell, 2011). The aim of these tasks is to validate that the researcher's findings and impressions correspond with the respondents' views (Bryman & Bell, 2011). Credibility could be achieved by providing each participant with an account of the researcher's observations and what was said during interview discussions (Bryman & Bell, 2011). Hence, after conducting and compiling the interviews for this study, the results were shared with each participant. Participants were notified that they could either confirm the information, reject it, or suggest alternative formulations. Although such participant validation potentially increases the research credibility, Bryman and Bell (2011) point out that researchers should not presume that participants can validate an analysis directed toward academics. Censorship problems could further arise if researchers provide influential groups, such as senior managers, with control of the research (Bryman & Bell, 2011). Since the results of this study were based on a single-case study involving only one case company, senior managers at the case company were concerned with anonymity. Therefore, senior managers at the case company were asked to validate and approve the results, potentially decreasing credibility as some information required being more anonymized.

3.3.2 Transferability

Transferability refers to demonstrating whether the findings of one study can be applied in other contexts or to a wider population (Bryman & Bell, 2011; Graneheim & Lundman, 2004; Shenton, 2004). Shenton (2004) points out how the results generated from qualitative studies should be comprehended within the context of the specifically studied organization. To facilitate this comprehension, Bryman and Bell (2011) and Graneheim and Lundman (2004) propose that researchers should provide clear and rich details of the selection and attributes of research participants, the context and organizational culture, and the data collection and analysis process. Since this study was based on a single-case study requiring a high degree of anonymity, the information about the case company and its interviewed employees had to remain limited. However, a description of the case company, the industry it operates in, and the area of expertise for each participant were presented to enhance transferability possibilities. Furthermore, the results chapter of this study includes a relatively extensive amount of data along with quotations from interviewees, which Graneheim and Lundman (2004) also suggest increases transferability. Since the results obtained through qualitative research are specific to the particular studied organization, Shenton (2004) raises challenges in achieving more general transferability. However, by conducting similar projects in different settings employing the same methods, a higher degree of transferability could potentially be validated (Shenton, 2004). Hence, by using the interview guide presented in Appendix 1 as a data collection tool, further studies could test the concepts of this study in other settings to enable a higher degree of transferability.

3.3.3 Dependability

Dependability addresses whether similar results would have been obtained if the work was repeated following the same research process, in the same context, and with the same research participants (Bryman & Bell, 2011; Shenton, 2004). This study has sought to provide transparency in the problem formulation, research participant selection, data collection, and data analysis processes to enable other researchers to obtain similar results. Bryman and Bell (2001) and Shenton (2004) argue that researchers could achieve dependability through such reporting of processes, actions, and choices made during the study.

3.3.4 Confirmability

Confirmability refers to demonstrating objectivity of the research by ensuring that the results reflect research participants' experiences rather than the researcher's individual preferences (Bryman & Bell, 2011; Shenton, 2004). Different measures were taken throughout this study to reduce the potential influence of bias and enhance confirmability. For instance, interviewee participants with different hierarchical positions and various backgrounds were selected to limit the risk of role-dependent biases and increase the potential for diverse answers. However, complete objectivity in qualitative research is difficult to ensure (Bryman and Bell, 2011; Shenton, 2004). For instance, in this study, the interview topics were designed and determined in advance to fit with the focus of the study, potentially reflecting the researcher's biases. More interviews could have been conducted with diverse employees at the case company to increase the confirmability of this study. Furthermore, interviews with other organizations in similar

contexts could have been conducted to broaden the scope of the study and reduce the risk of organizational bias.

3.4 Research Ethics

Ethical concerns typically arise during different research stages and should not be ignored (Bryman and Bell, 2011). Four areas to consider concerning ethical issues include the evaluation of potential harm to research participants, a lack of informed consent, an invasion of privacy, and deception (Bryman and Bell, 2011). The involvement of research participants in this study has been voluntary. At the beginning of the interviews, participants were informed about the purpose of the study and the reasons why their contributions were considered valuable. Participants were informed about the anonymity of individual participants, the case company, and sensitive topics to reduce stress and make participants feel comfortable sharing their personal experiences and information. Furthermore, participants were informed about the applied research process in advance before confirming their participation to prevent a lack of informed consent and deception. When conducting the interviews, participants were notified that they had the opportunity to withdraw their consent at any time or refuse to answer questions considered sensitive or personal to avoid an invasion of privacy.

4. Results

This chapter presents the results of the study. The results are exclusively based on insights obtained during data collection through interviews with employees at the case company. First, the main opportunities perceived by third-party payment product distribution through payment facilitators are presented. Second, the various topics that should be considered related to financial crime along with such partnerships are outlined. Finally, the chapter provides identified solutions for how considerations related to financial crime when partnering with third-party payment facilitators for payment product distribution could be managed.

Since the research questions of this thesis focused on understanding how fintech companies are affected by risks related to financial crime and how these can be managed, the interviews mainly dealt with topics that should be considered related to these risks. The opportunities of payment product distribution through third parties was only briefly discussed to provide context and gain a strategic perspective on why the case company uses such partnerships.

4.1 Opportunities of Third-Party Distribution

All interviewees agreed that there are multiple advantages of entering partnerships and using external payment facilitators for payment product distribution. The most frequently discussed opportunities involve the ability to scale at speed and gain control of the internal operational cost base while focusing on other business-critical areas.

4.1.1 Scaling

When asking participants about the opportunities related to using third parties for payment product distribution, all interviewees agreed that one of the main advantages involves the possibility of achieving more frictionless global scaling while making payment methods more accessible for merchants on multiple platforms globally. Interviewee K highlighted that a challenge for merchants is that they need to offer many payment methods to serve different types of consumers. Payment facilitators enable merchants to implement multiple payment options around the globe through a single contract and one integration. The interviewee underlined, "*From a merchant perspective, no one wants to do hundreds of integrations – you want one simple and straightforward integration and one contract to cover multiple payment methods for your customers.*" Hence, the interviewee described how payment product distribution through payment facilitators serves all actors in the ecosystem by solving challenges for all the parties involved. Interviewee D further noted, "*Scaling and onboarding a high number of new merchants require frictionless onboarding processes, both from an internal operational perspective as well as for the merchant experience.*" Hence, by leveraging the infrastructure and existing user bases of merchants that payment facilitators have created, the interviewee perceived an opportunity to frictionlessly onboard a high volume of merchants, promoting the ability to scale at speed.

4.1.2 Focused Operational Activities

Interviewees with legal, risk management, and business development expertise raised how acquiring new merchants internally and achieving global scale require solid procedures for underwriting and onboarding, including KYC, and managing the relationships with merchants. These processes were perceived as critical from a risk management perspective and for the merchant experience. However, interviewees D, E, and J pointed out that underwriting and onboarding processes require extensive operational work and are expensive to build and maintain over time. Interviewee J mentioned, "*Performing underwriting of each merchant you have a relationship with is expensive. You need access to the right data sources and people who will spend time doing it. Using a third party for these tasks enables you to grow faster with fewer resources.*" Hence, one frequently raised advantage of using payment facilitators for payment product distribution was the possibility to outsource the underwriting, onboarding, and direct relationships with a large number of merchants while gaining a higher control of the internal operational cost base. Interviewees F and J mentioned that rather than onboarding all the merchants that want to integrate your payment products, you only need to underwrite, onboard, and maintain the relationship with one payment facilitator that covers the financial risk related to merchants.

Multiple interviewees underlined that many payment facilitators have developed solid underwriting and KYC procedures. Payment facilitators have further specialized in offering good experiences for merchants by using simple, accessible, and streamlined onboarding processes while enabling the integration of a wide range of payment options for their consumers. Therefore, when outsourcing these activities to payment facilitators instead of managing them internally, interviewees acknowledged the opportunity to improve the merchant experience while being able to focus on other business-critical areas with the most internal expertise. Interviewee D highlighted, "*You should focus on doing the things that you are really good at while you let someone else do the things they have the most expertise in.*" All interviewees described how partnerships with payment facilitators could reduce the friction and work involved with having direct relationships with merchants, making internal operations more simple and focused. For instance, interviewee A underlined, "*Using someone in the middle can remove friction while making your job more focused. The middleman takes care of managing the relationships with merchants, while you just need to make sure that you manage the relationship well with the middleman.*" Hence, it was perceived as more scalable to use an intermediary actor to take care of areas related to merchants, such as KYC and AML, while only managing the relationships with payment facilitators rather than their whole merchant bases. As interviewee J noted, "*When using payment facilitators for payment product distribution, you need to ensure a good relationship only with these partners, rather than micro-managing each merchant, which could be beneficial in the long term.*"

4.2 Considerations Related to Financial Crime

Besides the perceived advantages of payment product distribution through third-party payment facilitators, participants also mentioned several topics when asked about the areas that should be considered related to financial crimes along with these partnerships. This section presents the most frequently discussed areas that should be considered, including increased dependency

on payment facilitators to mitigate financial crime, risk appetite alignment, fraud detection complexity, operational costs for managing financial crime and end consumer errands, and legal, reputational, and credit risks. Figure 4.1 illustrates a summary of the identified areas to consider.

Areas For Consideration	Examples
Third-Party Dependency	Value created dependent on payment facilitators Less insights into merchants that use your payment services Need for trust in partners Demand for mutually beneficial partnerships
Risk Appetite Alignment	Agreement on which merchants payment facilitators onboard Payment facilitators operating under other legal requirements Not fully transparent risk appetites Measures if agreed risk appetite is not followed
Fraud Detection Complexity	Difficulties in identifying fraudulent merchants Insufficient data points provided by payment facilitators
Operational Costs	Managing disputes and customer service related to fraud Dealing with end consumers Lengthy process to assess payment facilitators prior to entering partnerships
Legal Risk	Perceived negligence from regulators if payment facilitators have insufficient controls Indirect and involuntary facilitation of payments with criminal nature
Reputational Risk	Brand damage due to discreditable payment facilitator behavior Difficulties in covering reputational risk in contracts Misbehaving merchants damaging brand perception
Credit Risk	Payment facilitators might become financially weak Risk of having to repay end consumers for purchases through fraudulent merchants

Figure 4-1: Summary of identified areas to consider related to financial crime.

4.2.1 Third-Party Dependency

All interviewees agreed that using payment facilitators for merchant onboarding and payment product distribution increases the dependency on third parties. When performing these activities internally, interviewee D explained how the value created for merchants and end consumers depends only on you as a payment service provider. However, when using payment facilitators as intermediaries, the value creation becomes dependent on these third parties. Although interviewees pointed out the advantages of only needing to maintain a relationship with payment facilitators rather than with multiple merchants, interviewees with risk management and legal expertise underlined that one consequence could be that you do not know the merchants as well as you otherwise would do. Interviewee J noted, "*When you distribute your payment methods through external payment facilitators, you must be able to*

trust that the partner takes responsibility to keep the risk of onboarded merchants sufficiently low." Hence, multiple interviewees raised a need for trust in the payment facilitators you partner with to manage their merchant base correctly and take sufficient action to reduce financial crime risks.

As payment facilitators have direct relationships with merchants and are responsible for the merchant bases, interviewees E, H, and J explained that these partners could decide how and to which merchants they distribute their packages of payment services. Interviewee A described how the supply chain works similarly in most industries. The interviewee noted, "*If a company manufactures a car, and another company distributes and sells it, the manufacturer does not have a direct relationship with the end consumer; the manufacturer is not concerned with who the distributor sells the car to. However, when it comes to financial services and risks related to financial crime, it becomes more sensitive. You must ensure that you are confident in trusting your partners to do their job and take responsibility.*" Hence, multiple interviewees raised the importance of trusting and ensuring that the payment facilitators you partner with have implemented proper checks before onboarding merchants and allowing them to use your payment methods. Furthermore, interviewees D and G underlined how partnerships must be mutually beneficial for all parties involved when collaborating with external actors for payment product distribution, potentially creating challenges.

4.2.2 Risk Appetite Alignment

A majority of interviewees pointed out that different risk appetite levels could make it hard to agree on which types of merchants payment facilitators should onboard and distribute payment services to. Interviewees A, C, and D underlined that although most fintech companies operate more or less under the same laws and legal frameworks, they can choose their range within the legal bounds in which to operate. Interviewees D and K mentioned that there will always be risks related to fraud in fintech, but each company can choose its willingness to accept certain risks. Interviewee D noted, "*Each company sets its own risk appetite, and it becomes a matter of how much risk it is willing to accept within what is legal.*"

Interviewee J mentioned that several payment facilitators might accept payments for merchants that operate in more high-risk industries beyond your internal risk appetite. Furthermore, payment facilitators based in other markets with different regulatory requirements might naturally accept more risk than your risk appetite allows. Hence, it was considered critical to align on risk appetite levels and what types of merchants payment facilitators onboard and distribute payment products to in advance. However, interviewee A noted how the risk appetite levels partners set might not always be fully transparent. The interviewee pointed out a risk that payment facilitators communicate one level of risk appetite but practically do not follow it. There could further be situations where these partners agree on a risk appetite but are unable to effectively adhere to such an agreed-upon risk level. Hence, one challenge lies in ensuring that the partner complies with the agreed risk appetite and monitoring that they only onboard the merchants you want to use your payment products. Defining the consequences when a partner, for any reason, fails to adhere to the predefined risk appetite was perceived as critical by many interviewees. However, interviewee F emphasized that agreeing on potential measures

and actions to take along with the timelines for mitigation could be challenging to define in advance.

4.2.3 Fraud Detection Complexity

Several interviewees highlighted how using an intermediary actor for payment product distribution could make it harder to identify fraudulent merchants. If detecting a fraudulent merchant who onboarded through a specific payment facilitator and suspending it from using your payment services, interviewee D noted that there could be a risk that the merchant tries to onboard through another payment facilitator. Unless you have sufficient data points on the merchant, the interviewee pointed out that it could be hard to identify that it is the same fraudulent merchant. Interviewee D further mentioned, "*A critical challenge with financial crimes for all fintech companies is that after you learn how to detect a certain kind of fraud, and some time passes, criminals will create new ways of committing fraud.*" The interviewee underlined that new technology and methods using artificial intelligence make fraud increasingly sophisticated and complex, requiring increasingly faster and refined actions for detection.

4.2.4 Operational Costs

Interviewees D, E, G, and H noted that partnering with payment facilitators who onboard a high volume of fraudulent merchants could create additional time-consuming and costly operational work. Although the financial risk should be managed by payment facilitators, the operational costs related to managing customer service errands might still be managed internally. Interviewee D mentioned that if consumers do not receive items ordered through a fraudulent merchant, they may create disputes that must be dealt with internally. Interviewee H underlined, "*Fraud becomes bad because one knock-on effect is that we get disputes and errands from shoppers about it.*" If you identify a fraudulent merchant and know that the end consumers will not receive their orders, you must further figure out how to deal with these consumers. Additionally, interviewee H pointed out that payment facilitators that do not have proper controls to mitigate fraud create additional manual work as internal teams might be required to investigate and manage the issue.

Multiple interviewees highlighted that the underwriting of payment facilitators might require more manual work than the underwriting of individual merchants. For instance, interviewee C noted that assessing payment facilitators could be a lengthy process and more challenging since you need to take more factors into account. Interviewee E emphasized the need to assess the financial standing of payment facilitators and the merchants they onboard. If a payment facilitator has onboarded only a few merchants, and one is fraudulent, the interviewee mentioned that the payment facilitator becomes more dependent on this merchant than if they had a higher volume of their merchant base. Therefore, interviewee E underlined that entering into partnerships with payment facilitators could require a higher workload for onboarding, as the underwriting needs to include a more in-depth analysis of the financial standings of the payment facilitator and its merchant base.

4.2.5 Legal Risk

Interviewees with legal and risk management expertise raised how partnerships with payment facilitators could create legal risks if not correctly managed. From a theoretical perspective, interviewees B, C, and E pointed out that payment facilitators are liable for to which merchants they distribute payment products. However, as the payment service provider, you might, to some extent, be held accountable. Interviewees B, C, and I mentioned that various countries have different regulations and could have less robust AML programs on the governmental level. Hence, payment facilitators from such countries might have a bigger room for maneuver to not perform some of the checks expected to be done in the jurisdictions with more robust programs to combat financial crime. If you decide to partner with these actors despite being aware of their lack of controls, either due to the fact that they come from a less regulated country or that they themselves have poor AML programs, several regulators may perceive you as negligent. Interviewee B underlined, "*If you know a payment facilitator has less robust KYC or AML processes, yet you enter into a partnership with them, regulators might perceive this as negligence or failure to adapt proper risk assessments and measures.*" Although regulators might not hold you accountable to the same extent as the payment facilitator, interviewees noted that regulators might perceive your controls as weak. As interviewee J highlighted, "*If you would indirectly or involuntarily be part of a money laundering scheme, you could receive negative attention from regulators as your processes would seem weak.*" Interviewee B further mentioned that several countries, such as the US, have stricter regulations for facilitating payments with sanctioned individuals. The interviewee noted that if you partner with a payment facilitator that does not perform sufficient sanction checks and still let them distribute your payment services to anyone, you might facilitate payments with a sanctioned individual or company. If you are aware that such risks exist and do nothing about it, the interviewee noted that you might, to some extent, be held accountable by regulators.

4.2.6 Reputational Risk

All interviewees discussed an inherent risk of reputational damage when distributing payment products through external payment facilitators. Multiple interviewees provided examples of how indirect and involuntary criminal transaction involvement could damage your brand. For instance, apart from being a legal risk, interviewee J mentioned how involvement in a money laundering scheme could create reputational risks. Interviewee B referred to the misconduct of the German payment processor and financial services provider Wirecard, which is suspected to have engaged in money laundering and fraud practices, leading to insolvency in 2020 (McCrum et al., 2020). The interviewee further noted, "*If a scandal blows up, your brand might be on the first page everywhere as the payment provider whose services were used to finance a terrorist attack.*" Interviewee A said, "*Reputation does not care if something is legal or not, or even if it is true. If things come up on the Internet, you will be judged by them regardless of whether they are true or not, and that affects your reputation.*" Interviewees A and E mentioned that third-party contracts could be set up to recover financially in case of fraud, putting financial risk on payment facilitators. However, setting up contracts with these partners to protect you from reputational damage could be more challenging.

Interviewees discussed the reputational risk if your payment services would be visible on the websites of misbehaving merchants. For instance, interviewee B pointed out that consumers

who use your payment services to pay for their online orders might have a feeling that they are dealing with your company. However, they are dealing with the merchant of a payment facilitator with whom you have a partnership. Since end consumers might sense that they are doing business directly with you as a payment service provider, there is a reputational risk if the merchant does not deliver the goods. Hence, interviewee B emphasized that partnering with a payment facilitator with a large base of fraudulent merchants would not look good from the end consumer's point of view. Interviewees stressed how customers might associate their poor experiences from these purchases with your brand. Interviewee I noted, "*Merchants that commit fraud have a negative impact on end consumers. If you are associated with fraud, it damages consumers' perception of your brand.*" Interviewee D mentioned that you should consider the potential imbalance of having a few misbehaving merchants versus how many consumers they reach. If fraudulent merchants reach many consumers, your brand, PR, and reputation could be affected, which impacts your ability to scale and grow as a business.

4.2.7 Credit Risk

Several interviewees described how payment facilitators that onboard fraudulent merchants potentially create credit risks. If you are comfortable with the financial standing of a payment facilitator, interviewees D, E, and F noted that you might not need to worry too much about how financially strong the merchants they onboard are since this partner will cover their financial risk. Interviewee E mentioned that, theoretically, this could enable you to take on higher-risk merchants without being financially impacted, which could be helpful for several merchant segments that you would otherwise have a higher risk exposure toward. However, if the payment facilitator would become financially unable due to insolvency or, for any reason, would not cover the financial risk related to fraudulent merchants, interviewee E emphasized how this could create credit risks for you as a payment service provider. For instance, if consumers do not receive the goods they ordered through a fraudulent merchant, they might need to be repaid. In this case, if the payment facilitator is not able to repay the consumers, you, as a payment service provider, might need to assume liability of the refund regardless of if you already transferred the money to the payment facilitator.

Interviewees D and E discussed how credit risks increase for merchants that sell intangible products, such as travel events, flight tickets, and accommodation. The events often do not happen until several weeks, months, or years after the consumers placed and paid for their orders. Interviewee E mentioned that when noticing that a payment facilitator is very dependent on a high-risk or financially weak merchant or is financially deteriorating, the exposure could be mitigated or reduced by increasing the payment delay towards the payment facilitator. However, although there is some expectation that you must protect yourself to some degree according to your risk appetite, the interviewee noted that such solutions could create friction between these partners.

4.3 Risk Management

This section presents the identified solutions for how considerations related to financial crime when partnering with payment facilitators could be managed. First, interviewees perceived it as critical to set and align risk appetites, involve management in risk decisions, and perform

proper underwriting of payment facilitators before entering into partnerships. Second, after entering into partnerships with payment facilitators, controls in onboarding APIs, transaction monitoring, and key risk indicators (KRIs) could be used to detect financial crime patterns earlier and enable faster action for risk mitigation. Third, adaptive pricing strategies and fraud monitoring programs could be implemented to incentivize payment facilitators to adhere to the agreed risk appetite. Finally, data transfer agreements (DTAs) and robust contracts with payment facilitators could be set up to specify which data points payment facilitators should provide for financial crime detection and limit the exposure to financial crime risks. Figure 4.2 shows a summary of the identified solutions and their impact on the considered topics.

Partnership Stage	Solutions	Impact
Pre-Onboarding	**Define and Align Risk Appetites**	Internal alignment on acceptable risk levels Clarity on which payment facilitators to partner with Alignment with payment facilitators on acceptable risk levels
	Underwriting of Payment Facilitators	Insights into payment facilitators, their processes, and merchant bases Increased control of various risks Ensuring payment facilitators adhere to internal standards
Post-Onboarding	**Fraud Controls in Onboarding APIs**	Compliance with agreed risk appetite Early detection of financial crime patterns Immediate rejection of fraudulent merchants before onboarding Reduced pressure on payment facilitators during merchant onboarding Control over which merchants you have business with
	Transaction Monitoring	Compliance with agreed risk appetite Early detection of financial crime patterns Control over which merchants you have business with
	Key Risk Indicators	Compliance with agreed risk appetite Early detection of financial crime patterns Control over which merchants you have business with Transparency and collaborative approach to mitigating risks
	Adaptive Pricing	Compliance with agreed risk appetite Motivating payment facilitators to keep financial crime levels low Balancing risks for higher-risk segments
	Fraud Monitoring Programs	Compliance with agreed risk appetite Motivating payment facilitators to keep financial crime levels low Alignment on how fraud should be managed
Throughout Partnership	**Data Transfer Agreements**	Specifying data points that payment facilitators must share Access to sufficient data points for financial crime detection Consistency of data points provided by payment facilitators
	Robust Contracts	Compliance with agreed risk appetite Clarity on each party's obligations Limiting exposure to financial crime risks Enabling action if payment facilitators exceed risk appetite
	Management Involvement	Strategic decision-making for risk management

Figure 4-2: Identified solutions for how considerations related to financial crime could be managed and their impact on the considered topics.

4.3.1 Define and Align Risk Appetites

When partnering with payment facilitators for payment product distribution, interviewees C, F, G, I, J, and K emphasized that the first step to mitigating the risks related to financial crime is to set a risk appetite and then ensure alignment on it with partners. Interviewee K underlined,

"*There is no business without risks. You need to understand what the risks are for your business and take on the risks that make sense.*" Interviewees I and J especially mentioned the importance of defining and agreeing on an organizational risk appetite as you partner with external actors. Interviewee J highlighted, "*A well-defined risk appetite enables everyone involved in partnerships to understand what risks are acceptable versus too high and should be mitigated.*" Interviewees I and J further raised how the organizational risk appetite must be well-documented internally, as clarity on which risks you accept becomes increasingly critical as you scale. Interviewee I pointed out, "*For partnerships to work in a more scalable way, you must have a structure for how the risk appetite is defined, how escalations are managed, and which stakeholders should be involved if the risk appetite is exceeded. You must know what risk appetite you have and, based on that risk appetite, how you should mitigate various risks.*" Interviewee I further underlined, "*Clear guidelines on which risks you accept make it more clear which partners you can work with depending on their risk exposure in various markets and categories.*"

Apart from defining and agreeing on an internal risk appetite, all interviewees raised the importance of aligning risk appetite levels with partners. As companies can choose to be closer to the middle or the edge of what is legally required, aligning risk appetites before entering into partnerships was considered necessary. Interviewee K highlighted, "*When entering into partnerships, the risk appetite is critical for all the parties involved to understand each other.*" Hence, the importance of communicating your risk appetite and what fraud or dispute rates you deem acceptable toward partners was raised repeatedly during interviews.

4.3.2 Underwriting of Payment Facilitators

Apart from defining and aligning risk appetites and involving management in risk decisions, all interviewees pointed out the importance of performing proper underwriting of payment facilitators before considering a potential partnership. If performing appropriate KYC, AML, and due diligence on payment facilitators and managing those relationships well, interviewees A and B mentioned that you should cover the legal risk of these partnerships. Interviewee K further underlined the need to ensure that partners manage their responsibilities the way they should. Interviewees B, E, and F emphasized the importance of implementing a clear framework for assessing payment facilitators during onboarding and performing regular reviews of these partners.

Interviewee B explained how the Wolfsberg Group, consisting of 13 global banks that develop frameworks for managing financial crime risks (The Wolfsberg Group, 2018), has created a questionnaire for when banks partner with another financial institution. The interviewee mentioned that this questionnaire could be used as a reference and adapted to suit the purposes of partnerships with payment facilitators for payment product distribution. The interviewee explained that payment facilitators should be required to fill out the questionnaire before entering into partnerships to prevent financial crime risks. The interviewee raised KYC, licenses and legal background, fraud prevention and reporting, and financial counterparty risk as critical areas of information that the assessment of a payment facilitator should include before onboarding. Although payment facilitators own the relationships with merchants,

interviewees B and J noted that these partners should adhere to internal standards to let them distribute your payment services to the merchants they have business with.

Multiple interviewees mentioned that you need to perform sufficient checks to fully understand who the payment facilitator is and what they do, including confirming that the business exists, that they are performing well, and have no dealings with politically exposed persons. Furthermore, it must be understood what regulations the payment facilitator you partner with adhere to and what implications it has for your business. For instance, interviewee B noted that you must understand if the payment facilitator is a regulated company and, in that case, who supervises them. Furthermore, interviewees B and C mentioned that you should consider the legal requirements a partner operates under. Partnering with companies that have similar legal requirements was claimed to enable better governance of the partners and the controls they have in place. Hence, interviewee B highlighted that it could be beneficial to only partner with companies from countries with similar regulations and legal requirements to ensure that the partner has equivalent controls and will not pose any unnecessary risk. If a payment facilitator is from a different country that lacks regulations and legal requirements, the interviewee mentioned that your payment services might be distributed to people with whom you do not want to do business.

Interviewees with legal, risk management, and business development expertise raised it as critical to understand the procedures that payment facilitators use for onboarding new merchants, such as what information they collect, how they verify the identity of their customers, and how they perform AML risk assessment and scoring. Furthermore, it was considered necessary to assess how these partners work with fraud prevention and reporting to understand how they detect fraud, monitor the merchants to which they distribute payment services, and escalate suspicious transactions to authorities. Hence, the interviewees stressed the importance of ensuring that partners have proper controls and processes for KYC, AML, and due diligence to guarantee that your payment products will not be abused. Interviewee B mentioned that the monitoring systems partners have implemented to detect money laundering and fraud should be understood. The interviewee noted that payment facilitators should have policies that ensure they meet the global requirements for AML programs. For instance, if entering a partnership with a smaller payment facilitator in Asia that onboards merchants worldwide, you should ensure that their AML policy covers the global requirements. As interviewee B mentioned, "*We need to ensure that the partner understands how the global banking system works and what the global standards are*." In the same way, if a payment facilitator wants to operate in the US, the interviewee noted that you must ensure that they have US-based instruction policies and fully understand the requirements for this market.

Interviewee B noted that most payment facilitators are legally required to report suspicious activities to authorities. Therefore, it must be understood whether the partner has the required knowledge related to transaction monitoring and who is responsible for the reporting. To ensure that financial crime is taken seriously, the interviewee pointed out that it is critical to confirm that not only a partner's compliance department is responsible for and involved in risk management but also its senior management or owners. Furthermore, you must ensure that if suspicious activity is reported to senior management, they have the right staff to deal with the problem, such as AML analysts and a compliance team. The interviewee pointed out that you

should not expect other business functions to have sufficient money laundering or fraud knowledge. Hence, you must ensure that employees with the required knowledge can oversee these functions.

Apart from assessing payment facilitators, interviewees A, B, D, and E pointed out the importance of collecting data on their merchant bases during onboarding. Interviewee B mentioned that payment facilitators should communicate their share of merchants for different AML risk classes to understand the exposure to money laundering risks through a potential partnership. The interviewees further raised the necessity to consider the merchant mix of payment facilitators during onboarding to ensure you are not too exposed to one particular segment. For instance, interviewee E mentioned the need to identify the percentage of exposure or sales volume processed through the largest merchants of a payment facilitator. If a payment facilitator has a high concentration of a particular segment above a certain threshold and is reliant upon only a few merchants within this segment, the interviewee explained that the associated risks, including credit risk, must be considered. Additionally, partners should confirm that they will share necessary data upon request. For instance, interviewee B underlined that you must ensure that partners adhere to the laws of keeping their data records of merchants for a certain period and can share transaction data for due diligence if regulators request it or investigations need to be performed on merchants with whom they do business.

Several interviewees explained how performing background checks on publicly available information could be beneficial to complement the information shared by payment facilitators. Interviewee B noted that you must be able to trust that partners are honest and provide you with the correct information. However, sometimes the information you request partners to share may be publicly available. By asking payment facilitators to share their details, you could test if the partners are being honest with you. For instance, interviewees B and C noted that you could perform checks to confirm that payment facilitators previously were not fined by regulators for deficiencies or lack of function controls.

Overall, all interviewees described a thorough assessment of payment facilitators before entering into partnerships as critical. As interviewee K stressed, "*You should not enter into a serious business partnership with a partner that you do not know.*" Multiple times, it was raised how necessary checks during underwriting must be performed to comfortably enter into relationships and ensure that regulators do not perceive you as negligent. Additionally, performing these assessments was perceived as critical to reducing other negative consequences potentially created by partnerships with payment facilitators, such as reputational risks. Interviewee A underlined, "*You should probably care more and go beyond what you are required to do by law to ensure that your partners keep the risk low.*"

4.3.3 Fraud Controls in Onboarding APIs

After entering into partnerships with payment facilitators, multiple interviewees emphasized the importance of ensuring that these partners comply with the agreed risk appetite and monitoring that they only onboard the merchants you want to use your payment products. Interviewees D, F, I, and J highlighted that fraud controls could be implemented in onboarding APIs when merchants onboard through payment facilitators. When distributing payment

products and onboarding new merchants through payment facilitators, the underwriting and quality assurance of onboarded merchants is managed by these partners instead of internally. Consequently, rather than improving the underwriting process of merchants, interviewees D, F, and I underlined that such partnerships require an increased focus on early detection of potential fraud patterns.

Interviewees D and F highlighted how it might be helpful to perform internal fraud controls when merchants try to onboard to use your payment services. The onboarding API could include a preliminary fraud risk assessment to determine a merchant's fraud risk score by receiving specific non-transactional data points when the merchant onboards through a payment facilitator. If a merchant exceeds a specific fraud risk score, the API could reject them immediately from onboarding to use your payment services. However, interviewees D, F, and H pointed out how the idea of using payment facilitators partly is to make the onboarding process for merchants more efficient to promote increased transaction volumes, market penetration, and scaling. Implementing fraud controls in onboarding APIs could create more friction for merchants and negatively impact their experience during onboarding while requiring partners to share additional data points related to the merchants. Interviewees D and F underlined that it becomes an act of balance since you want the onboarding process for merchants to be as frictionless as possible and not require too many data points while receiving sufficient merchant data to detect fraud patterns and limit your exposure to financial crime. Interviewee H noted, "*Being able to onboard quickly with a payment facilitator is great from a user perspective. However, from our perspective, improper checks during onboarding could mean a higher risk exposure to fraudulent merchants*."

Interviewees D and F highlighted how partnerships with payment facilitators should decrease internal manual work related to KYC, underwriting, and regulatory requirements related to merchants. Therefore, fraud controls in the onboarding APIs require automated solutions to ensure that manual operational work does not increase. Interviewee F pointed out that the controls must be accurate to immediately reject merchants from onboarding and using your payment services without manual intervention. The interviewee further underlined that the main advantage of implementing automated controls in onboarding APIs is the ability to detect fraud before it happens. Since the quality of onboarded merchants lies with the payment facilitator, your leverage to reduce fraud rates and improve onboarding controls are limited. By implementing fraud controls in the onboarding APIs, the interviewee emphasized the possibility of reducing the pressure on payment facilitators while increasing the control over which merchants you have business with.

4.3.4 Transaction Monitoring

Apart from controls in the onboarding APIs, transaction monitoring for early fraud detection was frequently mentioned to monitor the risk exposure and ensure that payment facilitators comply with the agreed risk appetite after onboarding. Interviewee I pointed out, "*Rather than monitoring each merchant that uses your payment services, you need to monitor that the payment facilitator follows what you agreed on.*" Through transaction monitoring, interviewees raised how fraud could be detected earlier, enabling faster action for risk mitigation. Interviewee F mentioned that the data points collected in onboarding APIs could also be

utilized as a fraud risk indicator within early detection transaction monitoring. Furthermore, after onboarding payment facilitators and letting them distribute your payment services, several interviewees mentioned how automatic checks could be implemented to confirm that partners continue to follow the agreed standards. For instance, interviewee B highlighted that payment facilitators are contractually not allowed to distribute payment services in certain prohibited countries. To confirm that payment facilitators follow these restrictions, it could be beneficial to monitor which countries they distribute the payment services to and implement automatic alerts in case there still would be transactions in these countries. Apart from monitoring transactions in more high-risk markets, interviewee C noted that fraud rates, financial exposure, and the category of merchants that specific payment facilitators target could be monitored.

4.3.5 Key Risk Indicators

During transaction monitoring, interviewees C, F, and G pointed out the benefits of implementing key risk indicators (KRIs) for monitoring suspicious activities from payment facilitators' merchant bases. For instance, KRIs could be used for tracking fraud rates and the exposure to various risks. The interviewees highlighted that KRIs should be defined based on risk appetite, included in regular reviews, and monitored to ensure that acceptable risk levels are not exceeded. If the KRIs exceed satisfactory levels, you must begin looking into the problem and take action. Interviewees C and G mentioned that you need to start a conversation with the partner to understand the root cause of why the metrics look the way they do before taking appropriate action.

Interviewees F, G, and H emphasized that KRIs should continuously be shared with payment facilitators to enable transparency and a collaborative approach to mitigating risks. For instance, interviewee G mentioned that dashboards for tracking KRIs could be used to enhance transparency and the visibility of segments that are more exposed to financial crime, such as money laundering or fraud. The interviewee underlined how increased visibility and tracking of KRIs could enable you to be proactive and approach partners to identify improvement areas more collaboratively. As interviewee G pointed out, "*Being transparent with how you measure the performance of partners and acting on risks proactively through communication is better than just assuming that the partner already has the information and takes the right actions.*" Interviewee H further noted, "*You must communicate with partners to make them understand if their processes do not seem to work properly. By sharing your insights, they could learn something from you.*"

4.3.6 Adaptive Pricing

Besides ensuring compliance with the agreed risk appetite through controls in onboarding APIs, transaction monitoring, and KRIs, interviewees emphasized how an adaptive pricing strategy could be implemented to incentivize payment facilitators to adhere to the agreed risk appetite. Interviewee K pointed out, "*If you want someone to do something, it is quite traditional – you could use a carrot and a stick to drive a certain behavior. A carrot could motivate some kind of behavior through a positive reward, while a stick could be used if things do not go as the parties have agreed.*" In a business context, the interviewee further highlighted that the "carrot" is often in the form of money. The interviewee underlined, "*Financial compensation is the only language that businesses, and especially when companies are*

working together, really understand. The bottom line of businesses is often that either you make more money or you make less." Hence, several interviewees mentioned the possibility of adapting price levels to respond to the risk exposure toward different payment facilitators while motivating them to keep their financial crime levels low. Prices could increase for payment facilitators and merchants that use your payment services in more high-risk industries or markets, where financial crime is knowingly more common or hard to detect, to balance the higher risk. For instance, interviewee J mentioned that prices could be set depending on the risk you put yourself at. The interviewee pointed out, "*If you know that the risk is higher for a merchant, you should have sufficient margins to reflect this higher risk.*" In the same way, interviewees A, D, J, and K mentioned that price reductions or other rewards could be implemented as an incentive for the payment facilitators you partner with if they behave or perform better than expected.

Rather than setting price levels depending only on the geographic locations of merchants, interviewees D and J noted that you could be more granular to set individual prices based on more specific industries or business markets. However, interviewee D emphasized that such a classification of merchants requires payment facilitators to share the relevant data to enable the identification of these merchant categorizations.

4.3.7 Fraud Monitoring Programs

Along with an adaptive pricing strategy, the implementation of fraud monitoring programs to incentivize payment facilitators to adhere to the agreed risk appetite was discussed. Interviewee J underlined, "*Fraud monitoring programs could function as an incentive for partners not to onboard fraudulent merchants.*" Interviewee G further highlighted, "*By implementing a fraud monitoring program, you could show that you are on top of things and do not just let transactions happen.*" Interviewees mentioned that you could have different thresholds for fraud levels that trigger various actions if exceeded. For instance, interviewee C pointed out that you could implement a three-step framework: 1) early warning threshold, 2) excessive threshold, and 3) termination. The interviewee mentioned that you should be clear about what measures you will take if you see that a payment facilitator exceeds any of these steps.

Once having identified that merchants under a specific payment facilitator exceeded an early warning threshold for fraudulent transactions and concluded that there is something wrong on the payment facilitator's end, interviewee C emphasized that you should start a communication to identify why they exceeded the threshold. It should be asked why the fraud rates are high and what could be the problem. The payment facilitator might need to check if it is a one-off problem or has been continuously happening for some time. Furthermore, interviewees noted that you could require the payment facilitator to create a remediation plan to fix the problem. After agreeing on a remediation plan and ensuring it is sufficient to solve the problem, interviewee C pointed out that you could follow up on the execution. While the payment facilitator executes the remediation plan, you could consider whether you need to implement additional controls to mitigate your risk exposure. For instance, you may want to cut off the transactions for the merchants they onboarded to use your payment services if the fraud rates increase at a certain speed. However, the interviewee noted that, although you can implement controls on your end, the root cause of the high fraud rates probably lies on the payment

facilitator due to poor merchant onboarding or a poor fraud mitigation strategy. Therefore, these partners should be responsible for fixing the root problem. The interviewee underlined, "*We are in the position to act and demand that partners fulfill their obligations.*"

If the remediation plan does not lead to sufficient improvement within a specified time, interviewees discussed the possibility of implementing penalties, such as fees. Interviewees D and F mentioned that fraud monitoring programs with potentially negative consequences for payment facilitators could be beneficial as it creates a mutual understanding of how fraud is defined and the importance of mitigating financial crime. However, several interviewees were skeptical about penalty fees as appropriate measures. Interviewee H noted, "*Yes, we could penalize partners, and yes, we could terminate merchants from using our services. However, that does not resolve the real issue, which is that the partner should be onboarding better merchants in the first place – we should not have to identify them.*" Interviewee I further pointed out, "*It could be challenging to implement high fees because it might negatively impact the relationships with payment facilitators while being expensive to push through if there would be a dispute around it.*" Interviewee G also underlined, "*I do not think you should necessarily put fines on partners, who you depend on for your own success. Rather than pushing penalties on partners who do not improve their fraud rates within a certain time, you could tell them that you will look into alternative approaches because you need to take action to compensate for your exposure to fraud.*" The interviewee explained that you should instead focus on having a good connection and relationship with the partner to manage such situations through conversations and a collaborative approach. However, although penalties could be bad for business relationships with payment facilitators, interviewee C stressed that it might be necessary to ensure improvement.

Interviewee D pointed out that fraud monitoring programs with potential penalty fees require negotiation with payment facilitators when forming contracts; "*Naturally, no one wants to sign a contract that could entail fees*." However, since other influential actors, such as Visa and MasterCard, have similar programs with penalties if fraud levels exceed certain thresholds, interviewee D underlined that implementing penalties might not be perceived by partners as unreasonable. On the other hand, interviewee A highlighted, "*The tricky part of comparing yourself with Visa or Mastercard is that they are extremely powerful in the industry. They are these giants that everyone has to comply with – they can basically create any program that looks in any way, and then everyone else will just accept it.*" The interviewee noted that other companies with less influence than these actors need to ensure that such programs make sense to partners. Interviewee J mentioned that while you expand and grow your business, it might be hard to implement programs with penalty fees as potential consequences. Interviewee A further pointed out, "*While it might seem like a good idea in principle, you need to face reality and actually understand whether it is something the partners can implement or would be interested in implementing.*"

All interviewees agreed that the best solution would be to solve the problem before you have to implement penalties. As interviewee D emphasized, "*You probably do not want to get to the stage where you put penalty fees on the partner. Hopefully, you have a relationship with the partner where you work collaboratively to reduce fraud.*" Interviewees D and K further raised that fraud should not be in the interest of payment facilitators since they are losing money on

it and getting attention from regulators and authorities. Interviewee D said, "*No one wants fraud because it is bad for everyone involved except for the fraudster.*" Therefore, it should be in their best interest to fix it as soon as possible. Interviewee I pointed out, "*If a payment facilitator distributes payment products to fraudulent merchants, they are put at both financial and legal risk. Additionally, since these partners are losing money in case of fraud, it should be in their interests to decrease their fraud rates.*" Interviewee B further underlined that most payment facilitators would probably improve their fraud rates before reaching the stage where fines are imposed, especially since detailed checks are performed on partners before entering into the partnerships. From previous experience, the interviewee had the perception that payment facilitators, in general, are open to conversations about compliance in case of financial crime, are often transparent with their transaction monitoring processes when requested, and provide details if necessary. In previous situations, interviewee B described how partners had been willing to improve their fraud rates upon request since they had already received regulators' attention and needed to improve their processes regardless.

Rather than implementing fraud monitoring programs to earn money, multiple interviewees noted that the purpose of such programs should be to have a discussion with partners and align on how fraud should be managed. For instance, interviewee F raised that the main advantages of implementing a fraud monitoring program include making payment facilitators' responsibilities to mitigate financial crimes clear and ensuring alignment on risk appetites. The obligation of partners to create remediation plans if the levels of financial crime for the merchants they onboard exceed the agreed risk appetite provide security while enabling greater control of which merchants have access to your payment services. If you see no improvement from the remediation plan, interviewees raised how you need to decide if you are comfortable still taking on the risk from the partnership. Interviewee C underlined that it should be up to management to decide whether the reputational risk, increased operational costs, and regulator obligations that a continued partnership with the payment facilitator might require are reasonable from a business strategy perspective. If the risk of continuing the partnership with a payment facilitator exceeds your risk appetite, the interviewee pointed out that you might potentially need to terminate the relationship.

Since partners have several months to improve their processes through remediation plans, interviewee F highlighted that fraud monitoring programs could enable a more long-term solution as it likely takes several months before financial crime levels improve sufficiently. In contrast to implementing extra controls in onboarding APIs, fraud monitoring programs could provide a solution for keeping the onboarding process for merchants as efficient as possible while keeping payment facilitators obliged to maintain low financial crime levels. However, from a financial crime perspective, it was mentioned that the optimal solution could be to combine such programs with implementing controls in onboarding APIs and continuous transaction monitoring. Interviewee F pointed out, "*Fraud monitoring programs could enable long-term solutions as partners work to improve their processes for several months. However, complementing such programs with automated, internal fraud controls through onboarding APIs and transaction monitoring could enable you to act fast and mitigate risks more short-term.*" Hence, by combining all these methods for financial crime prevention, interviewee F emphasized that both short- and long-term solutions could be achieved to limit the exposure to financial crime created by partnerships with payment facilitators.

4.3.8 Data Transfer Agreements

The possibilities of detecting and managing fraud through controls in onboarding APIs, transaction monitoring, KRIs, fraud monitoring programs, and adaptive pricing are dependent on having sufficient data points on merchants and their transactions. Hence, interviewees with risk management expertise raised the importance of implementing data transfer agreements (DTAs) that specify which data points payment facilitators are required to provide for financial crime detection. For instance, interviewee D pointed out that having the right data points could increase the possibility of detecting previously terminated merchants that try to onboard again through a different payment facilitator. Furthermore, data on payment facilitators' merchant bases could be used to detect collusion fraud easier, where a merchant and consumer collaborate to trick the system and commit fraud. If suspecting that a merchant is fraudulent, the interviewee mentioned that it may be helpful to request additional data from partners to confirm the suspicions. However, as the business grows, requesting data ad-hoc after suspecting a merchant as fraudulent might be too late and not a scalable solution. Hence, interviewees D, F, and J emphasized the need for a standardized solution across all the payment facilitators you partner with for which data points they should be required to share to ensure scalability and restrict the customization requirements within the fraud detection setup.

Interviewee D pointed out that data points related to merchants are part of the payment facilitators' customer registers, which they might not want to let go of. Hence, asking payment facilitators for too many data points might not be possible. The interviewee explained that while extra merchant data could be used to improve the experience for consumers by protecting them from fraud and bad actors, payment facilitators might seek to protect their merchants by not sharing too much data. Different payment facilitators might further have different integrations with your payment services, which could make data sharing technically complex. Additionally, several data points that you request might not yet be collected by some payment facilitators. Interviewee F underlined that the possibility of receiving extra merchant data depends on what type of data points you need, which type of payment facilitator you partner with, their access to the data points, and the technical limitations in their integration.

Interviewees D, F, and J highlighted that DTAs could be complex and hard to establish. If a partner is resistant to sharing extra merchant data necessary for your internal fraud prevention program, interviewee F mentioned that the first step should be to understand the reason. Second, you need to be clear about your use case and how the partner also could benefit from collecting and sharing the data points. The interviewee pointed out that there might be a need to push the partner to understand that the same data could be critical for them to mitigate their risks by enabling better risk monitoring for fraud prevention. Hence, you should make payment facilitators understand that they also would benefit from collecting the data points by clearly explaining the use cases and demonstrating a mutual benefit.

4.3.9 Robust Contracts

All interviewees agreed that implementing robust contracts with payment facilitators is critical to limit the exposure to risks related to financial crime created by these third-party relationships. In business models where multiple parties need to agree on something, interviewee K noted that one challenge is for everyone to agree on alignment as different parties

see things differently. The interviewee pointed out, "*The more parties you add, sometimes the more challenging it becomes to find a common ground. You need to align on how you are offering something, what the terms of conditions of the partnership are, and how you are going to work together.*" Hence, interviewees D, F, I, J, and K emphasized that contracts should clearly state the agreed risk appetite and what risks you accept. To manage risks related to fraud, interviewees D, I, and K highlighted that it is critical to have the same view of when something is considered fraud, how fraud should be measured, and who should do something about it. Therefore, contracts with payment facilitators must include the definition of such financial crime activities and acceptable fraud levels. As interviewee I underlined, "*The methods and requirements for risk mitigation should be clearly stated in the contracts with partners.*"

Interviewee F pointed out that contracts with payment facilitators should ensure that you have the possibility to act fast, have the right to transfer claims back to the partner in case of financial crime, and make the information exchange for financial crime investigations as efficient as possible. Since payment facilitators are intermediaries for the distribution of payment products, the interviewee emphasized that you must have contracts that state how the end consumers will be affected in case of disputes related to financial crime. For instance, contracts must declare how end consumers will be affected and how long they will need to wait until receiving their refunds in case of fraud. Consumers will submit the disputes to the financial service provider, who then transfers the claim to the payment facilitator, who finally contacts the merchant. Hence, interviewee F raised how the contracts must clearly state each party's obligations. Interviewees F and J further highlighted that contracts should include the data points that you require payment facilitators to share for purposes of transaction monitoring. Hence, including DTAs in the contracts with partners that specify the required data points for early fraud detection was perceived as critical.

Interviewees D, F, and J mentioned how contracts could be adapted according to the internal risk appetite. The interviewees further raised the importance of documenting the potential consequences of financial crime that exceed the agreed risk appetite in writing. For instance, in case of high fraud rates, the contracts could state how payment facilitators could be prohibited from onboarding new merchants until they fix the problem while being obliged to update you continuously on their progress. Interviewee D underlined that contracts should state potential penalties, such as fees, if payment facilitators exceed the agreed risk appetite. Interviewee H further highlighted that in the case of fraud, contracts could include the right to disassociate yourself from fraudulent merchants that the payment facilitator onboarded by rejecting them from using your payment methods.

Interviewee J mentioned that you could have base pricing applied to all the payment facilitators you onboard. However, for adaptive pricing strategies, contracts could state how pricing levels regularly might update to reflect different risk levels. The interviewee emphasized, "*The different price levels for the corresponding risk levels should be transparent, clearly stated in contracts, and communicated to partners in advance.*" Interviewee A agreed that contracts could include clauses that state how the pricing will update based on specific metrics, such as fraud levels or dispute rates. Furthermore, interviewee D highlighted that contracts could include clauses to limit payment product distribution for specific high-risk industries, product

segments, or markets. When establishing new partnerships with payment facilitators, contracts could also include specific measures until the payment facilitators have proven to be reliable partners. For instance, interviewee D mentioned the possibility of having a two-factor verification obligation for merchants onboarding through a new payment facilitator until they reach specific transaction volumes and prove their reliability of rejecting fraudulent merchants from onboarding. Finally, interviewees I and J stressed that contracts should state your right to perform regular audits on the payment facilitators you partner with to confirm that their processes adhere to the agreed standards.

4.3.10 Management Involvement

Multiple interviewees emphasized the involvement of management in managing various risks as critical. Interviewee J raised that, in the end, it should be up to management to strategically decide which risk appetite you have and which risks you are comfortable taking. Interviewee C emphasized, "*Risk management needs attention from management. If you see risks, you should be able to escalate these and suggest mitigation actions to management. Then, management can decide whether they feel comfortable accepting the risks.*" Interviewee J further pointed out, "*Employees with risk expertise could present potential risks and their consequences to management. However, in the end, management should be responsible for deciding whether the risk should be mitigated and accepted, or ultimately rejected.*"

5. Analysis

This chapter presents an analysis of the obtained results related to the theoretical framework presented in Chapter 2. The research questions of this study aimed to answer how risks related to financial crime affect fintech companies that provide online financial services when collaborating with third-party actors in business ecosystems for payment product distribution and how these risks could be managed. Hence, the analysis mainly focuses on the identified considerations related to these topics obtained from the results, compared and contrasted with theories related to business ecosystems and financial crime in the payment industry.

5.1 Increased Value for End Consumers

Based on the interviews, fintech companies that provide online financial services could benefit from enhanced scaling opportunities by reaching new merchants, consumers, and markets by collaborating with third-party payment facilitators. By using payment facilitators as intermediary actors for payment product distribution, merchants could benefit from enhanced value creation through simplified integration of new payment products. The incentives for merchants to integrate payment products were, in turn, driven by changing customer preferences involving the ability to choose between multiple payment options for online purchases. Hence, the opportunity for online financial services providers to scale their businesses by partnering with third-party payment facilitators could be explained as an impact of enhancing the value creation for end consumers, which studies indicated as critical for successful business ecosystem outcomes (Moore, 2006; Zahra & Nambisan, 2012). Figure 5.1 illustrates how online financial services providers can enhance the value for end consumers through partnerships with third-party payment facilitators.

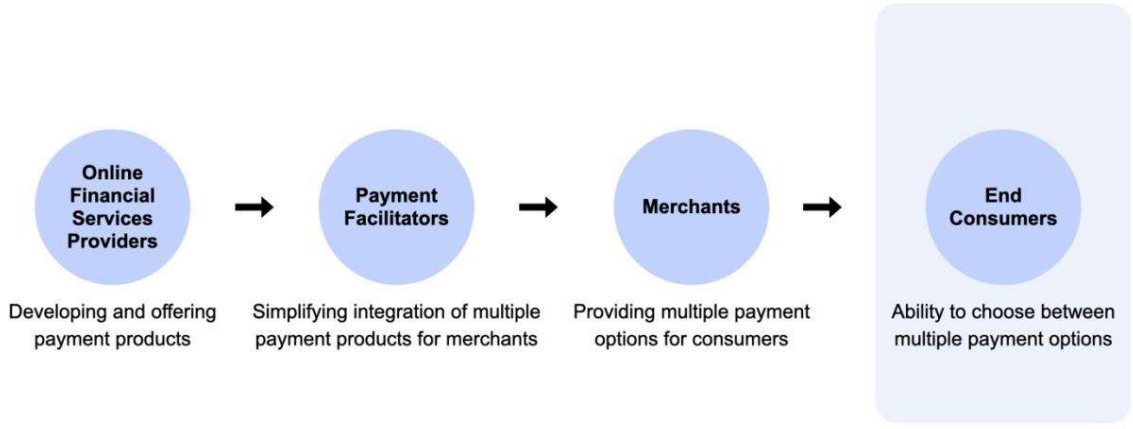

Figure 5-1: Illustration of how online financial services providers enhance the value for end consumers through partnerships with third-party payment facilitators.

5.2 Complexity of Changing Dynamics

Apart from promoting business opportunities, the results showed that risks related to financial crime demand that online financial services providers consider multiple topics when partnering with third-party payment facilitators for payment product distribution to manage these risks. For instance, online financial services providers should consider increased third-party dependency on payment facilitators to mitigate financial crime risks, risk appetite alignment, fraud detection complexity, operational costs for managing financial crime and end consumer errands, and legal, reputational, and credit risks. Studies showed that shifting competitive dynamics and cooperation processes could add complexity to decision-making processes for companies participating in business ecosystems (Ramezani & Camarinha-Matos, 2020; Zahra & Nambisan, 2012). Hence, the opportunities for online financial services providers to partner with third-party payment facilitators for competitive advantages while considering risks related to financial crime along with these partnerships could be related to these theories.

5.3 Effects of Third-Party Dependency

The interviews emphasized that partnerships with payment facilitators increase third-party dependency for online financial services providers as the value created for merchants and end consumers becomes dependent on payment facilitators. At the same time, payment facilitators depend on online financial services providers to offer payment products to the merchants they have relationships with. This third-party dependency corresponds with theories on how companies participating in business ecosystems depend on each other for shared value-creation and to reach common strategic objectives (Kapoor, 2018; Kim et al., 2010; Ramezani & Camarinha-Matos, 2020; Rong et al., 2015). Furthermore, based on the results, multiple topics which online financial services providers should consider related to financial crime risks when collaborating with payment facilitators could be related to this increased third-party dependency. For instance, the need to consider risk appetite alignment and legal and reputational risks could be explained as an effect of the increased dependency on payment facilitators. These results indicate that third-party dependency and its effects become critical to consider when partnerships involve risks related to financial crime.

Interviews confirmed that managing financial crime risks becomes increasingly challenging as criminals use new, more sophisticated methods, aligning with studies on financial crime (e.g., Chapelle, 2019; Giudici, 2018; Sullivan, 2010; Zetzsche et al., 2020). Hence, one consideration related to third-party dependency involves how the possibilities for online financial services providers to detect fraud depend on the data exchange with payment facilitators. Business ecosystem participation could enable companies to navigate changing market dynamics (Clarysse et al., 2014; Zahra & Nambisan, 2012). Therefore, partnerships with payment facilitators could arguably enhance the possibilities of managing fraud risks through collaboration in the dynamic risk landscape of the payment industry. However, the results showed that insufficient data exchange with payment facilitators could limit the possibilities for online financial services providers to catch fraudulent merchants and transactions. For instance, collaboration could suffer from issues related to the data exchange between these partners, as online financial services providers need sufficient data points from payment facilitators to detect fraud. These issues correspond with the challenges of managing

technological problems in business ecosystems, such as the rules for data exchange among ecosystem members, creating barriers to achieving coordinated memberships (Lenkenhoff et al., 2018).

The opportunity for online financial services providers to cost-effectively focus on business-critical areas with the most internal expertise aligns with how business ecosystems could enable companies to explore business opportunities with less time and resources in-house (Fuller et al., 2019). However, despite this opportunity, the results showed that the actions performed by payment facilitators could affect the costs and profitability of online financial services providers. For instance, operational costs could increase if payment facilitators distribute payment products to fraudulent merchants. These effects could be related to how cooperation could suffer if the profits generated through a business ecosystem are not fairly distributed among members (Immonen et al., 2014), requiring attention to reduce friction between partners. Furthermore, a system built of multiple components could increase the risks of bottlenecks, limiting growth and demand and affecting the ecosystem value proposition through cost, performance, or scarcity constraints (Kapoor, 2018). Apart from affecting internal operational costs for online financial services providers, the results indicated that payment facilitators that onboard fraudulent merchants negatively impact the end customer experience. Hence, the bad customer experience from fraud could decrease the total value created in the business ecosystem while negatively affecting online financial services providers through consequences such as reputational damage.

5.4 Collaboration

Studies indicated that challenges in business ecosystems, such as third-party dependency, could be managed partly by achieving successful collaboration between members (e.g., Koenig, 2013; Moore, 2006; Ramezani & Camarinha-Matos, 2020). The interviews confirmed this need for collaboration between online financial services providers and payment facilitators. Based on the results, transparency and continuous communication between online financial services providers and payment facilitators could promote successful business ecosystem collaboration and control various risks, aligning with business ecosystem studies (e.g., Koenig, 2013; Moore, 2006; Ramezani & Camarinha-Matos, 2020). Based on the interviews, online financial services providers could continuously share KRIs with payment facilitators to enable transparency and a collaborative approach to mitigating risks. By increasing the visibility and tracking of KRIs toward payment facilitators through shared dashboards, online financial services providers could be proactive and approach partners to identify improvement areas more collaboratively. This approach aligns with how studies indicated that individual companies should contribute with collaborative and creative attitudes, competencies, and engagement to support alignment and agreement in business ecosystems (Lenkenhoff et al., 2018). These measures could further be related to the initiatives presented in section 2.3.4.3, launched across card issuers to increase the protection of sensitive data and counterfeit payment fraud, where it was argued that security efforts within these networks should be pursued through collaboration (Sullivan 2010). Interviews also emphasized that fraud monitoring programs could facilitate discussions with partners and alignment on how fraud should be managed. Hence, online financial services providers could more easily manage financial crime risks through conversations and a collaborative approach by focusing on having a good connection and relationship with payment

facilitators. Studies showed that companies could struggle with collaboration as internal business needs distract members away from business ecosystem concerns (Moore, 2006). Therefore, online financial services providers could arguably achieve commitment from payment facilitators to support ecosystem concerns by implementing these measures for collaboration.

5.5 Partner Alignment and Agreement

Studies suggested that alignment and agreement between members in business ecosystems is necessary to achieve successful collaboration and business ecosystem outcomes (e.g., Adner, 2017; Immonen et al., 2014; Koenig, 2013; Lenkenhoff et al., 2018; Moore, 2006). Based on the results, online financial services providers could manage considerations related to financial crime when partnering with third-party payment facilitators by implementing measures for alignment and agreement, thus aligning with business ecosystem studies. Such measures include setting and aligning risk appetites, performing underwriting of payment facilitators, and implementing robust contracts, DTAs, fraud monitoring programs, adaptive pricing, and shared KRIs.

Before entering into partnerships, the results showed that online financial services providers should achieve alignment with payment facilitators by communicating their risk appetite and what fraud rates they deem acceptable. The importance of such alignment increased as the lines for financial crime risks could be unclear since different companies in the payment industry could choose to be closer to the middle or the edge of what is legally required. Different risk appetite levels could make it hard to agree on which types of merchants payment facilitators should onboard and distribute payment services to. These issues could be related to how various companies define their own strategies concerning ecosystem structure, roles, and risks, which could create contradiction rather than consistency (Adner, 2017). Furthermore, partnerships with payment facilitators with a higher risk appetite could increase the risk for online financial services providers that their payment products are distributed to fraudulent merchants, decreasing the value for end consumers who might suffer from fraud. These potential negative consequences for end consumers relate to how companies with different purposes and decision-making standards could cause risks of unintended business ecosystem outputs (Tsujimoto et al., 2018).

Based on the results, performing underwriting of payment facilitators could promote alignment by ensuring that online financial services providers only partner with actors that share a similar risk appetite. For instance, online financial services providers could confirm alignment on payment facilitators' procedures for merchant onboarding and fraud prevention. This alignment could promote agreement between members about shared project development and visions, supporting synergistic value-adding and mutually beneficial processes (Koenig, 2013; Lenkenhoff et al., 2018; Moore, 2006). Furthermore, the results showed that implementing robust contracts is necessary to ensure alignment on multiple aspects of partnerships with payment facilitators, such as how the financial services are offered, what the terms of conditions of the partnerships are, and how the partnership practically will work. Alignment through such protocols and interfaces for individual contributions, roles, and services, corresponds with how studies indicated that companies could achieve alignment with business

ecosystem members through such measures (Immonen et al., 2014; Moore, 2006). Additionally, interviews showed that DTAs could be implemented in contracts for rules on which data points payment facilitators should share for fraud detection and prevention and ensure efficient standards for data exchange. These standards align with how studies argued that the success of a business ecosystem depends on its rules of engagement, standards, and interfaces, such as requirements that participants agree to a minimal set of rules (Jacobides et al., 2018).

5.6 Incentives for Commitment and Adherence

Based on the results, online financial services providers should implement measures to support commitment and adherence to agreed risk levels. The need for such measures was illustrated in section 2.3.4.3 by the initiatives to combat fraud across card networks, where different members' incentives to make individual efforts compromised the entire network security, increasing dependency on the weakest links (Sullivan, 2010). For instance, online financial services providers could implement fraud monitoring programs with potential penalty fees and adaptive pricing strategies to incentivize payment facilitators to keep financial crime levels low. These measures align with how studies indicated that companies operating in business ecosystems could benefit from cost- and profit-sharing arrangements and a willingness to share their profits and risks to create fair mechanisms (Immonen et al., 2014; Ramezani & Camarinha-Matos, 2020). Hence, by implementing such measures, online financial services providers could get economic compensation for the increased risk exposure created by payment facilitators that do not adhere to the agreed-upon risk standards while enhancing commitment. However, in practice, the interviews showed that penalty fees could be hard to implement since such measures could harm the relationships with payment facilitators. Therefore, online financial services providers should arguably perform internal assessments to understand whether such efforts make sense and should be implemented. Figure 5.2 presents a summary of the theories on how business ecosystem challenges could be managed presented in Chapter 2 and corresponding measures identified in the results.

Business Ecosystem Theories	Results
Alignment and Agreement	Define and Align Risk Appetites Underwriting of Payment Facilitators Robust Contracts Data Transfer Agreements Adaptive Pricing Fraud Monitoring Programs
Sharing of Both Profits and Risks	Adaptive Pricing Fraud Monitoring Programs
Focus on Customer Value	Enhancing value for end customers through partnerships with payment facilitators

Figure 5-2: Theories on how business ecosystem challenges could be managed and corresponding measures identified in the results.

5.7 Coordination and Trust

Studies indicated that alignment and agreement are necessary to promote coordination in business ecosystems (e.g., Koenig, 2013; Moore, 2006; Ramezani & Camarinha-Matos, 2020). Apart from the ability to scale speedily, the interviews implied an opportunity to cost-

effectively focus on business-critical areas with the most internal expertise while outsourcing some functions to payment facilitators. This opportunity corresponds with how coordination in business ecosystems could enable companies to focus on managing the issues within their specific domains and invest their resources in more rapid internal innovation (Immonen et al., 2014; Moore, 2006). For instance, online financial services providers could increasingly focus on developing their payment product offerings while outsourcing distribution activities, such as KYC and underwriting of merchants, to payment facilitators. These opportunities align with how studies suggested that financial companies could fulfill regulatory requirements while improving the efficiency and operations of KYC by outsourcing such activities to third parties (Steinert & Williams, 2020). Studies on how KYC processes are becoming increasingly complex and incurring higher expenses (e.g., Berg et al., 2020; Chen, 2022; Gomber et al., 2017; Schlatt et al., 2022; Yadav & Chandak, 2019) further illustrate the opportunity for online financial services providers to outsource KYC processes. However, when outsourcing activities related to risk management, interviews emphasized the need to control issues related to payment facilitators' responsibilities to limit the exposure to financial crime risks. These controls contradict how the coordination in business ecosystems could enable companies to partially ignore the problems arising in external environments and reduce the need to manage interdependencies and uncertainties (Immonen et al., 2014; Moore, 2006). Rather than ignoring the problems arising in payment facilitators' domains, the results showed that online financial services providers should focus on ensuring that such issues do not occur in the first place. For instance, online financial services providers could implement fraud controls in onboarding APIs and transaction monitoring to continuously ensure that payment facilitators adhere to the agreed standards and limit the exposure to financial crime risks.

Section 2.3.4.3 presented how the actors involved in the mobile payment market, such as mobile device manufacturers, financial services providers, and telecommunication companies, should coordinate their efforts and collaborate to ensure the security of online payment environments (Bezovski, 2016; Sullivan, 2010). According to these theories, security problems should be solved through coordination instead of individual investments by companies in unneeded technology and separate systems for transaction monitoring and screening (Sullivan, 2010). Hence, these theories indicate that the internal control mechanisms proposed during interviews could be sub-optimal from a business ecosystem point of view. Furthermore, the theories imply that online financial services providers should aim to achieve sufficient coordination with payment facilitators rather than implementing internal measures, such as fraud controls in onboarding APIs and transaction monitoring. However, the need for internal control mechanisms presented in the results indicates that, in practice, it could be difficult for online financial services providers to achieve sufficient business ecosystem coordination due to the interdependence with payment facilitators and their activities. The need for such controls could further imply a lack of trust between business ecosystem members. Studies indicated that alignment is critical for trust-building among business ecosystem members (Lenkenhoff et al., 2018). Hence, similar to the issues in the mobile payment industry between various actors, the implied lack of trust could potentially be explained by difficulties in achieving alignment between online financial services providers and payment facilitators. Section 2.3.4.3 indicated that outsourced solutions for KYC could form conflicting initiatives between companies and their outsourcing partners, as partners might focus on capturing revenue from their products and services rather than creating value for the financial companies (Steinert & Williams, 2020).

This theory indicates a risk that payment facilitators, in some cases, might have a higher risk appetite and onboard merchants to optimize their revenues, potentially resulting in a higher volume of fraudulent merchants and reducing the trust of online financial services providers.

The interviews showed a risk that payment facilitators communicate one risk appetite but practically do not follow it or struggle with effectively adhering to the agreed-upon risk level. If failing to recognize such inconsistent strategies within a given period, business ecosystem members could suffer from non-convergent actions (Adner, 2017). The results showed that online financial services providers could face critical risks if payment facilitators do not adhere to the agreed standards regarding financial crime mitigation, such as increased legal, reputational, and credit risks. These results align with studies indicating that poor KYC policies and procedures could affect such risks (Rajput, 2013). Hence, trust may become increasingly difficult to establish when partnerships impact the exposure to various risks with potentially damaging consequences. Therefore, as the results showed, online financial services providers could arguably benefit from internal controls to limit their risk exposure created by payment facilitators' actions and decrease the need for trust. Through fraud controls in onboarding APIs and transaction monitoring, online financial services providers could control that payment facilitators adhere to the agreed standards to reduce their exposure to risks related to financial crime. Figure 5.3 presents the identified measures for ensuring that payment facilitators adhere to the agreed standards to limit the exposure to risks related to financial crime and the implications of the need for such measures.

Results	Implications
Fraud Controls in Onboarding APIs	Difficulties in achieving sufficient business ecosystem coordination due to interdependence
	Hard to establish sufficient trust and alignment between business ecosystem members
Transaction Monitoring	Trust becoming increasingly difficult when partnerships impact risks with damaging consequences

Figure 5-3: Measures for ensuring that payment facilitators adhere to the agreed standards to limit the exposure to risks related to financial crime and the implications of the need for such measures.

5.8 Management Involvement and Dynamic Risk Appetite

According to interviews, management should be responsible for strategically deciding the risk appetite and which risks they are comfortable taking. Studies further suggested that managers should determine a firm-wide risk appetite considering various issues, such as strategy, stakeholders' interests, risk capacity, business conditions, and the overall competitive environment (Gontarek & Bender, 2019). Hence, these requirements for considerations on a strategic level support the need for management involvement in risk decisions to define a risk appetite aligning with strategic objectives on the firm level.

In situations where the lines for risks are not clear, studies argued that companies need to apply a nuanced perspective built on objective facts when defining risk appetite and continuously update their views as their environment, fact base, and business model change (Jain et al., 2020; Rittenberg and Martens, 2012). These theories indicate that online financial services providers should aim to define a dynamic risk appetite when partnering with different payment

facilitators over time to manage the changing dynamics in the payment industry. However, applying a dynamic risk appetite could arguably create challenges for online financial services providers and the payment facilitators they partner with. For instance, interviews showed that online financial services providers should be clear about their internal risk appetite to enable an understanding of the risks that should be mitigated and promote clarity on which payment facilitators they should partner with. Hence, confusion could arguably arise within the organization if the risk appetite is continuously updated, while partnerships potentially could suffer from reduced clarity of which risks are accepted. The interviews showed that the internal risk appetite should be well-documented to allow organization-wide clarity and transparency, aligning with how Rittenberg and Martens (2012) highlighted the need to clearly communicate the risk appetite. Hence, it could be assumed that the need for such documentation increases when the risk appetite is continually updated to reflect the dynamic risk landscape. Furthermore, the need for continuous and transparent communication with payment facilitators arguably increases to avoid confusion and alignment complexity as the risk appetite updates.

6. Discussion

This study has contributed to several implications related to the studied issue relevant for theory and practitioners. First, this chapter presents a discussion of the theoretical and practical implications. Second, related recommendations for managers at fintech companies that provide online financial services are outlined. Finally, the chapter discusses the limitations of the obtained findings and suggestions for future research.

6.1 Theoretical Implications

Existing theories on business ecosystems and financial crime in the payment industry have been combined with empirical data from an increasingly emerging context that has previously been somewhat inaccessible to social science inquiry. Thereby, this study has contributed to theory by exploring how fintech companies that provide online financial services can manage risks related to financial crime when partnering with third-party actors in business ecosystems.

The study has identified that theories on business ecosystem challenges and how these could be managed are applicable to the risks related to financial crime that online financial services providers face when collaborating with third-party payment facilitators for payment product distribution. Aligning with existing theories on these topics (e.g., Kapoor, 2018; Kim et al., 2010; Ramezani & Camarinha-Matos, 2020; Rong et al., 2015), online financial services providers are affected by multiple risks due to the third-party dependency created by their partnerships. Moreover, online financial services providers could manage these risks by implementing measures for alignment and agreement to promote collaboration and coordination with such third parties. These measures correspond with existing theory on how business ecosystem challenges could be managed (e.g., Adner, 2017; Immonen et al., 2014; Koenig, 2013; Lenkenhoff et al., 2018; Moore, 2006). However, online financial services providers could benefit from complementing these measures with internal mechanisms to monitor that their partners adhere to agreed standards and control the risk exposure created by these partnerships. The need for these complementary measures confirm the difficulties for companies operating in business ecosystems to achieve sufficient alignment and trust to support fully coordinated memberships (e.g., Adner, 2017; Koenig, 2013; Lenkenhoff et al., 2018; Moore, 2006; Ramezani & Camarinha-Matos, 2020; Tsujimoto et al., 2018).

6.2 Practical Implications

The study has shown that online financial services providers are affected by risks related to financial crime in multiple ways when collaborating with third parties in business ecosystems for payment product distribution. Hence, one main contribution of this study for practitioners is a demonstration of the aspects related to financial crime risks that online financial services providers should consider along with these partnerships. Moreover, the study has presented actionable solutions for how practitioners could manage these risks. One main conclusion relevant for practitioners is that various solutions should be implemented pre-onboarding, post-

onboarding, and throughout the partnerships to manage the third-party dependency and its associated effects. Practitioners should focus on achieving alignment and agreement with partners to support collaboration and coordination for successful business ecosystem outcomes. Complementary measures for monitoring and controlling that partners adhere to agreed risk standards should further be implemented to limit the exposure to risks related to financial crime created by these partnerships.

6.3 Recommendations for Management

Managers at fintech companies that provide online financial services are recommended to use the findings of this study as a guide when evaluating strategic partnerships with third-party actors in business ecosystems. First, before entering into new partnerships, managers should define and communicate a firm-wide, dynamic risk appetite based on strategic firm objectives. Second, an understanding of how specific partnerships support the strategic firm objectives should be obtained. Third, managers are recommended to comprehend how the risks related to financial crime created by these partnerships affect their business and evaluate whether they conform to the risk appetite. Finally, managers need to identify which measures they could implement to control the risks exceeding the internal risk appetite. By doing so, managers should be able to effectively evaluate partnerships by balancing opportunities with risks while enabling more effective strategy formulation that supports strategic firm objectives. Figure 6.1 presents the recommended actions for managers and their impact when evaluating strategic partnerships with third-party actors in business ecosystems.

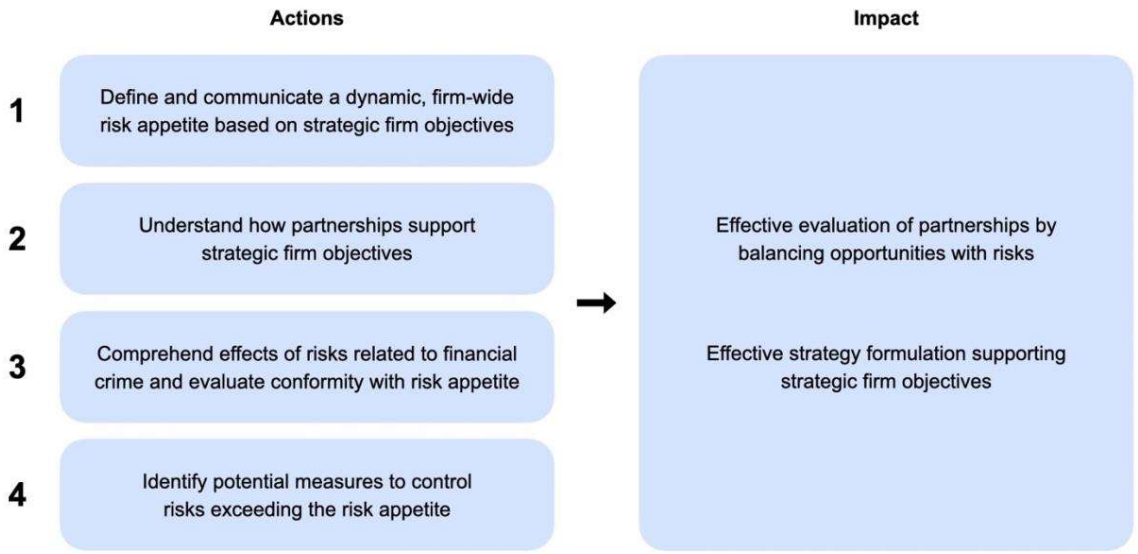

Figure 6-1: Recommended actions for managers of online financial services providers and their impact when evaluating strategic partnerships with third-party actors in business ecosystems.

6.4 Limitations

By performing a single-case study, this study has focused on particularization rather than generalization. Hence, the limitations of this study mainly relate to the generalizability of the obtained findings. By exploring the particular case, the study has focused on partnerships between fintech companies that provide online financial services and third-party actors for payment product distribution. Since the challenges related to financial crime and the changing dynamics in the payment industry are applicable across various companies in the payment industry, the results may apply to other financial companies in the payment industry apart from fintech companies. For instance, the effects related to financial crime and measures for managing these risks could apply to other financial companies offering online financial services and partnering with third-party actors for payment product distribution, such as credit and debit card companies. Furthermore, although this study has exclusively focused on collaboration with third-party actors in business ecosystems for payment product distribution, the findings may be relevant for financial companies that partner with third-party actors for other purposes. However, no conclusions regarding such generalization can be drawn from this study due to its focus on particularization.

6.5 Future Research

Future studies are recommended to validate the findings of this study by exploring the same issues within organizations other than the studied case company. For instance, other fintech companies that offer online financial services and partner with third-party actors for payment product distribution, similar to the case company, could be studied. Additionally, the same issues could be explored from the perspective of payment facilitators instead of online financial services providers to gain an additional perspective on the findings presented in this study. It is further proposed that future research investigates the studied issue in different settings to confirm the generalizability of the findings. First, future studies could analyze in more detail if the same results apply to other actors in the payment industry apart from fintech companies that provide online financial services, such as credit and debit card companies. Second, it could be explored whether the findings apply to partnerships between actors for purposes other than payment product distribution and, in that case, which types of partnerships this includes. For instance, future studies could explore whether the recommended actions for managers presented in Figure 6.1 applies to other forms of partnerships with a potential impact on risks related to financial crime and third-party dependency. Finally, future research could explore the possibilities of achieving sufficient coordination between actors in the payment industry that collaborate in business ecosystems in more detail. This study identified that online financial services providers could implement internal control mechanisms to limit the risk exposure created by their partnerships with third-party actors for payment product distribution. However, future studies could more deeply investigate the possibilities of instead achieving sufficient coordination and trust to reduce the need for these internal controls.

7. Conclusion

This study aimed to explore how fintech companies that provide online financial services can manage risks related to financial crime when partnering with third-party actors in business ecosystems for payment product distribution. First, to answer this aim, it was investigated how risks related to financial crime affect online financial services providers when partnering with third-party actors in business ecosystems for payment product distribution. Second, it was studied how online financial services providers could manage these risks.

The study identified that risks related to financial crime affect fintech companies that provide online financial services in multiple ways when partnering with third-party actors in business ecosystems. These effects mainly relate to the increased third-party dependency on external actors, including how the value created in business ecosystems becomes dependent on third-party actors and the need for trust in these partners to adhere to agreed risk standards. Moreover, third-party dependency impacts multiple other areas that online financial services providers should consider, including risk appetite alignment, fraud detection complexity, operational costs, and legal, reputational, and credit risks.

Multiple solutions for how fintech companies that provide online financial services could manage risks related to financial crime when partnering with third-party actors in business ecosystems have been proposed. First, measures could be implemented for alignment and agreement to promote collaboration and coordination, such as defining and aligning risk appetites, performing underwriting of partners, and implementing robust contracts, DTAs, and shared KRIs. Second, actions could be taken to incentivize adherence to the agreed risk standards, such as adaptive pricing strategies and programs with potential penalty fees. Arguably, since penalty fees could harm relationships with partners, alternative approaches should be taken if the effects of penalty fees damage the relationships with partners to the degree that collaboration suffers. Third, trust and coordination become increasingly difficult to establish when partnerships impact the exposure to various risks with potentially damaging consequences. Therefore, fintech companies could benefit from complementing these measures with internal mechanisms, such as fraud controls in onboarding APIs and transaction monitoring, to control and monitor that partners adhere to agreed risk standards and limit the risk exposure created by the partnerships. Finally, management should be involved in risk decisions and determine a dynamic risk appetite to respond to the changing dynamics in the payment industry along with these partnerships.

References

Adner, R. (2017). Ecosystem as structure: An actionable construct for strategy. *Journal of management*, *43*(1), 39-58. https://doi.org/10.1177/0149206316678451

American Express. (2023, April). *Payment Facilitator Acceptance of American Express® Cards*. https://www.americanexpress.com/en-us/business/optblue/agent/agent-resources/PaymentFacilitatorFactSheet.pdf

Apple. (n.d.). *Working with an E-Commerce Platform or a Payment Service Provider*. Retrieved March 26, 2023, from https://developer.apple.com/apple-pay/payment-platforms/

Arner, D. W., Zetzsche, D. A., Buckley, R. P., & Barberis, J. N. (2019). The identity challenge in finance: from analogue identity to digitized identification to digital KYC utilities. *European business organization law review*, *20*, 55-80. 10.2139/ssrn.3224115

Arner, D., Buckley, R., Charamba, K., Sergeev, A., & Zetzsche, D. (2022). Governing Fintech 4.0: Bigtech, Platform Finance, and Sustainable Development. *Fordham J. Corp. & Fin. L.*, *27*, 1. 10.2139/ssrn.3915275

Au, Y. A., & Kauffman, R. J. (2008). The economics of mobile payments: Understanding stakeholder issues for an emerging financial technology application. *Electronic commerce research and applications*, *7*(2), 141-164. https://doi.org/10.1016/j.elerap.2006.12.004

Autio, E., & Thomas, L. D. (2020). Value co-creation in ecosystems: Insights and research promise from three disciplinary perspectives. In *Handbook of digital innovation* (pp. 107-132). Edward Elgar Publishing. https://doi.org/10.4337/9781788119986.00017

Baldwin, C. Y. (2012). Organization design for business ecosystems. *Journal of Organization Design, 1*(1). https://doi.org/10.7146/jod.6334

Bryman, A., & Bell, E. (2011). *Business research methods* (3rd ed.). Oxford university press.

Berg, G., Guadamillas, M., Natarajan, H., & Sarkar, A. (2020). *Fintech in Europe and Central Asia: Maximizing benefits and managing risks*. The World Bank Group. https://pdfs.semanticscholar.org/a14a/280b99603c083a62e6d00f290c0d03349534.pdf

Bezovski, Z. (2016). The future of the mobile payment as electronic payment system. *European Journal of Business and Management*, *8*(8), 127-132.

Bolton, R. J., & Hand, D. J. (2002). Statistical fraud detection: A review. *Statistical science*, *17*(3), 235-255. 10.1214/ss/1042727940

Buehler, K. (2019). Transforming approaches to AML and financial crime. *McKinsey & Company*. https://www.mckinsey.com/~/media/mckinsey/business%20functions/risk/our%20insights/tra

nsforming%20approaches%20to%20aml%20and%20financial%20crime/transforming-approaches-to-aml-and-financial%20crime-vf.pdf

Chapelle, A. (2019). *Operational risk management: best practices in the financial services industry*. John Wiley & Sons.

checkout.com. (2023, January 11). *Fraud monitoring programs*. Retrieved March 26, 2023, from https://www.checkout.com/docs/risk-management/disputes/fraud-monitoring-programs#Visa's_Fraud_Monitoring_Program

Chen, J. (2022, August 4). *Know Your Client (KYC): What It Means, Compliance Requirements.* Retrieved March 26, 2023, from https://www.investopedia.com/terms/k/knowyourclient.asp

Chen, T. H. (2020). Do you know your customer? Bank risk assessment based on machine learning. *Applied Soft Computing, 86*, 105779. https://doi.org/10.1016/j.asoc.2019.105779

Cheng, M., & Qu, Y. (2023). Does Operational Risk Management Benefit from FinTech?. *Emerging Markets Finance and Trade*, 1-16. https://doi.org/10.1080/1540496X.2022.2164464

Chiodo, T. E., Cremo, N., Forsythe, J., Hyland, C., Orenbuch, M., & Zhang, C. (2021). *Payments, Processors, & FinTech: If Software Is Eating the World… Payments Is Taking a Bite*. Credit Suisse. https://research-doc.credit-suisse.com/docView?language=ENG&format=PDF&sourceid=em&document_id=1083376791&serialid=Xv39ocygAc3ZfJnVd7%2Bd46T7aoIwVSA1Nyw3xJ%2Fgi0o%3D&cspId=null

Clarysse, B., Wright, M., Bruneel, J., & Mahajan, A. (2014). Creating value in ecosystems: Crossing the chasm between knowledge and business ecosystems. *Research policy*, *43*(7), 1164-1176. https://doi.org/10.1016/j.respol.2014.04.014

Consumer Sentinel Network, *U.S. Federal Trade Commission Report* (2022).

Coskun, V., Ozdenizci, B., & Ok, K. (2013). A survey on near field communication (NFC) technology. *Wireless personal communications*, *71*, 2259-2294. 10.1007/s11277-012-0935-5

Deloitte. (2018). *FinTech: Regulatory Challenges and Financial Crime Exposure*. https://www2.deloitte.com/content/dam/Deloitte/de/Documents/finance/Deloitte_FinTech.pdf

Deloitte. (2021). *Realizing the digital promise: Transformation in an ecosystem of regulators, BigTech, Fintech and more*. https://www.deloitte.com/content/dam/assets-shared/legacy/docs/perspectives/2022/gx-realizing-the-digital-promise-transformation-in-an-ecosystem.pdf

Easton, G. (2010). Critical realism in case study research. *Industrial Marketing Management, 39*(1), 118-128. 10.1016/j.indmarman.2008.06.004

Eisenhardt, K. M. (1989). Building theories from case study research. *Academy of management review, 14*(4), 532-550. 10.2307/258557

Elliott, K., Coopamootoo, K., Curran, E., Ezhilchelvan, P., Finnigan, S., Horsfall, D., & van Moorsel, A. (2022). Know Your Customer: Balancing innovation and regulation for financial inclusion. *Data & Policy, 4*, e34. 10.1017/dap.2022.23

European Central Bank. (2018, March). *The revised Payment Services Directive (PSD2) and the transition to stronger payments security*. Retrieved May 15, 2023, from https://www.ecb.europa.eu/paym/intro/mip-online/2018/html/1803_revisedpsd.en.html

European Central Bank. (2022). *Study on New Digital Payment Methods*. https://www.ecb.europa.eu/paym/digital_euro/investigation/profuse/shared/files/dedocs/ecb.dedocs220330_report.en.pdf

Faccia, A., Moşteanu, N. R., Cavaliere, L. P. L., & Mataruna-Dos-Santos, L. J. (2020, September). Electronic money laundering, the dark side of fintech: An overview of the most recent cases. In *Proceedings of the 2020 12th international conference on information management and engineering* (pp. 29-34). 10.1145/3430279.3430284

Feyen, E., Frost, J., Gambacorta, L., Natarajan, H., & Saal, M. (2021). Fintech and the digital transformation of financial services: implications for market structure and public policy. *BIS Papers*. https://www.bis.org/publ/bppdf/bispap117.pdf

Fritz-Morgenthal, S., Huber, J. A., Funaro, D. (2018). Preventing Disaster: How Banks Can Manage Operational Risk. *Bain & Company*. https://www.bain.com/contentassets/f0199ad9887e402cb37cd1fd316f5ee3/bain_brief_how_banks_can_manage_operational_risk.pdf

Fuller, J., Jacobides, M. G., & Reeves, M. (2019). The myths and realities of business ecosystems. *MIT Sloan Management Review, 60*(3), 1-9. https://sloanreview.mit.edu/article/the-myths-and-...

Gancz, A., Halder, D., Bull, T., & Elinson, S. (2022). How the rise of PayTech is reshaping the payments landscape. *Ernst & Young*. https://www.ey.com/en_pl/payments/how-the-rise-of-paytech-is-reshaping-the-payments-landscape

Girling, P. X. (2022). *Operational Risk Management: A Complete Guide for Banking and Fintech*. John Wiley & Sons.

Giudici, P. (2018). Fintech risk management: A research challenge for artificial intelligence in finance. *Frontiers in Artificial Intelligence, 1*, 1. 10.3389/frai.2018.00001

Global Payments. (2022). *2022 Commerce and Payment Trends Report*. https://docs.globalpaymentsinc.com/v/2022-commerce-and-payment-trends-report-en

Gomber, P., Koch, J. A., & Siering, M. (2017). Digital Finance and FinTech: current research and future research directions. *Journal of Business Economics, 87*, 537-580. 10.1007/s11573-017-0852-x

Gontarek, W. (2016). Risk governance of financial institutions: The growing importance of risk appetite and culture. *Journal of Risk Management in Financial Institutions, 9*(2), 120-129. academia.edu/26238650/Risk_governance_of_...

Gontarek, W., & Bender, R. (2019). Examining risk governance practices in global financial institutions: the adoption of risk appetite statements. *Journal of Banking Regulation, 20*, 74-85. 10.1057/s41261-018-0067-2

Gozman, D., & Willcocks, L. (2019). The emerging Cloud Dilemma: Balancing innovation with cross-border privacy and outsourcing regulations. *Journal of Business Research, 97*, 235-256. 10.1016/j.jbusres.2018.06.006

Graça, P., & Camarinha-Matos, L. M. (2017). Performance indicators for collaborative business ecosystems—Literature review and trends. *Technological Forecasting and Social Change, 116*, 237-255. 10.1016/j.techfore.2016.10.012

Graneheim, U. H., & Lundman, B. (2004). Qualitative content analysis in nursing research: concepts, procedures and measures to achieve trustworthiness. *Nurse education today, 24*(2), 105-112. 10.1016/j.nedt.2003.10.001

Grasshoff, G., Coppola, M., Gehra, B., Kampmann, K., Pfuhler, T., Uhlmann, P., A., & Wiegand, C. (2021). Global Risk 2021: Building a Stronger, Healthier Bank. *Boston Consulting Group*. https://www.bcg.com/publications/2021/embracing-change-post-pandemic-in-the-banking-industry

Grodal, S., Anteby, M., & Holm, A. L. (2021). Achieving rigor in qualitative analysis: The role of active categorization in theory building. *Academy of Management Review, 46*(3), 591-612. 10.5465/amr.2018.0482

Gupta, S. (2013). The mobile banking and payment revolution. *European Financial Review, 2*(36), 215254. hbs.edu/ris/Publication%2520Files...

Gupta, R., Mejia, C., & Kajikawa, Y. (2019). Business, innovation and digital ecosystems landscape survey and knowledge cross sharing. *Technological Forecasting and Social Change, 147*, 100-109. 10.1016/j.techfore.2019.07.004

Gupta, D., Polkowski, Z., Khanna, A., Bhattacharyya, S., & Castillo, O. (2022). *Proceedings of Data Analytics and Management*. Springer Singapore. 10.1007/978-981-16-6289-8

Guthrie, J. (n.d.). What is a Payfac? *Mollie*. Retrieved May 16, 2023, from https://www.mollie.com/growth/what-is-a-payfac

Guo, J., & Bouwman, H. (2016). An analytical framework for an m-payment ecosystem: A merchants′ perspective. *Telecommunications Policy, 40*(2-3), 147-167. 10.1016/j.telpol.2015.09.008

Hanelt, A., Bohnsack, R., Marz, D., & Antunes Marante, C. (2021). A systematic review of the literature on digital transformation: Insights and implications for strategy and organizational change. *Journal of Management Studies, 58*(5), 1159-1197. 10.1111/joms.12639

Hasham, S., Joshi, S., & Mikkelsen, D. (2019). Financial crime and fraud in the age of cybersecurity. *McKinsey & Company*. https://www.mckinsey.com/~/media/McKinsey/...

Hayes, A. (2023, January 29). *Apple Pay*. Retrieved March 26, 2023, from https://www.investopedia.com/terms/a/apple-pay.asp

Henningsson, S., & Hedman, J. (2014). Transformation of digital ecosystems: The case of digital payments. In Information and Communication Technology: Second IFIP TC5/8 International Conference, ICT-EurAsia 2014, Bali, Indonesia, April 14-17, 2014. Proceedings 2 (pp. 46-55). Springer Berlin Heidelberg. 10.1007/978-3-642-55032-4

Hoch, N. B., & Brad, S. (2021). Managing business model innovation: An innovative approach towards designing a digital ecosystem and multi-sided platform. *Business Process Management Journal, 27*(2), 415-438. 10.1108/BPMJ-01-2020-0017

Hutchings, A., & Holt, T. J. (2015). A crime script analysis of the online stolen data market. *British Journal of Criminology, 55*(3), 596-614. 10.1093/bjc/azu106

International Monetary Fund. (2001). Financial System Abuse, Financial Crime and Money Laundering—Background Paper.

Iman, N. (2018). Is mobile payment still relevant in the fintech era?. *Electronic Commerce Research and Applications, 30*, 72-82. 10.1016/j.elerap.2018.05.009

Immonen, A., Palviainen, M., & Ovaska, E. (2014). Requirements of an open data based business ecosystem. IEEE access, 2, 88-103. 10.1109/ACCESS.2014.2302872

Jacobides, M. G., Cennamo, C., & Gawer, A. (2018). Towards a theory of ecosystems. *Strategic management journal, 39*(8), 2255-2276. 10.1002/smj.2904

Jain, R., Nauck, F., Poppensieker, T., & White, O. (2020). Meeting the future: Dynamic risk management for uncertain times. *McKinsey & Company*. https://www.mckinsey.com/capabilities/risk-and-resilience/our-insights/meeting-the-future-dynamic-risk-management-for-uncertain-times

Jullum, M., Løland, A., Huseby, R. B., Ånonsen, G., & Lorentzen, J. (2020). Detecting money laundering transactions with machine learning. *Journal of Money Laundering Control, 23*(1), 173-186. 10.1108/JMLC-07-2019-0055

Jung, K. B., Kang, S. W., & Choi, S. B. (2020). Empowering leadership, risk-taking behavior, and employees' commitment to organizational change: The mediated moderating role of task complexity. *Sustainability, 12*(6), 2340. 10.3390/su12062340

J. P. Morgan. (2021). *Key Trends to Drive Your Payments Strategy*. https://www.jpmorgan.com/content/dam/jpm/merchant-services/insights/e-commerce/key-trends-to-drive-your-payments-strategy.pdf

J. P. Morgan. (2022a). *Visa Dispute & Fraud Monitoring Programs Guide*. https://www.jpmorgan.com/content/dam/jpm/merchant-services/documents/payment-network-updates/VDMP-VFMP_ProgGuide_02092022.pdf

J. P. Morgan. (2022b). *Mastercard Excessive Fraud Merchant (EFM) Program: Frequently Asked Questions*. https://www.jpmorgan.com/content/dam/jpm/merchant-services/documents/payment-network-updates/MC_ExcessiveFraud_FAQ_02092022.pdf

Kallio, H., Pietilä, A. M., Johnson, M., & Kangasniemi, M. (2016). Systematic methodological review: developing a framework for a qualitative semi-structured interview guide. *Journal of advanced nursing, 72*(12), 2954-2965. 10.1111/jan.13031

Kapoor, R. (2018). Ecosystems: broadening the locus of value creation. *Journal of Organization Design, 7*(1), 1-16. 10.1186/s41469-018-0035-4

Karadag, B., Akbulut, A., & Zaim, A. H. (2022, November). A Review on Blockchain Applications in Fintech Ecosystem. In *2022 International Conference on Advanced Creative Networks and Intelligent Systems (ICACNIS)* (pp. 1-5). IEEE. 10.1109/ICACNIS57039.2022.10054910

Khan, B. U. I., Olanrewaju, R. F., Baba, A. M., Langoo, A. A., & Assad, S. (2017). A compendious study of online payment systems: Past developments, present impact, and future considerations. *International journal of advanced computer science and applications, 8*(5). 10.14569/IJACSA.2017.080532

Koenig, G. (2013). Business ecosystems revisited. *Understanding Business Ecosystems: How firm Succeed in the New World of Convergence, Brussels, De Boeck*, 69-83. https://www.researchgate.net/publication/288449196_Business_Ecosystems_Revisited

Kou, G., Olgu Akdeniz, Ö., Dinçer, H., & Yüksel, S. (2021). Fintech investments in European banks: a hybrid IT2 fuzzy multidimensional decision-making approach. *Financial Innovation, 7*(1), 39. 10.1186/s40854-021-00256-y

Lee, I., & Shin, Y. J. (2018). Fintech: Ecosystem, business models, investment decisions, and challenges. *Business horizons, 61*(1), 35-46. 10.1016/j.bushor.2017.09.003

Leong, C., Tan, B., Xiao, X., Tan, F. T. C., & Sun, Y. (2017). Nurturing a FinTech ecosystem: The case of a youth microloan startup in China. *International Journal of Information Management, 37*(2), 92-97. 10.1111/jan.13031

Li, Y. R. (2009). The technological roadmap of Cisco's business ecosystem. *Technovation, 29*(5), 379-386. 10.1016/j.technovation.2009.01.007

Liu, J., Kauffman, R. J., & Ma, D. (2015). Competition, cooperation, and regulation: Understanding the evolution of the mobile payments technology ecosystem. *Electronic Commerce Research and Applications, 14*(5), 372-391. 10.1016/j.elerap.2015.03.003

Loukoianova, E., Davidovic, S., Sullivan, C., & Tourpe, H. (2019). Strategy for Fintech Applications in the Pacific Island Countries. *IMF APD Departmental Paper*, *19*, 14. 10.5089/9781498326735.087

Malhotra, D., Saini, P., & Singh, A. K. (2022). How blockchain can automate KYC: systematic review. *Wireless Personal Communications*, *122*(2), 1987-2021. 10.1007/s11277-021-08977-0

Mastercard. (n.d.). *Find a payment facilitator*. Retrieved May 15, 2023, from https://www.mastercard.us/en-us/business/overview/start-accepting/payment-facilitators.html

Matzler, K., Friedrich von den Eichen, S., Anschober, M., & Kohler, T. (2018). The crusade of digital disruption. *Journal of Business Strategy, 39*(6), 13-20. 10.1108/JBS-12-2017-0187

McCrum, D., Storbeck, O., Palma, S., & Reed, J. (2020, June 25). *Wirecard collapses into insolvency*. Retrieved May 3, 2023, from https://www.ft.com/content/ac949729-6167-4b6c-ac3f-f0aa71aca193

McKinsey & Company. (2020). *McKinsey on Payments* (12/30). https://www.mckinsey.com/~/media/McKinsey/Industries/Financial%20Services/Our%20Insights/McKinsey%20on%20Payments%2030/McK_on_Payments_30.ashx

Mention, A. L. (2019). The future of fintech. *Research-Technology Management, 62*(4), 59-63. 10.1080/08956308.2019.1613123

Mikkelsen, D., Rajdev, S., & Stergiou, V. (2022). Managing financial crime risk in digital payments. *McKinsey &* Company. https://www.mckinsey.com/capabilities/risk-and-resilience/our-insights/managing-financial-crime-risk-in-digital-payments

Milian, E. Z., Spinola, M. D. M., & de Carvalho, M. M. (2019). Fintechs: A literature review and research agenda. *Electronic Commerce Research and Applications, 34*, 100833. 10.1016/j.elerap.2019.100833

Moore, J. F. (2006). Business ecosystems and the view from the firm. *The antitrust bulletin, 51*(1), 31-75. 10.1177/0003603X0605100103

Murinde, V., Rizopoulos, E., & Zachariadis, M. (2022). The impact of the FinTech revolution on the future of banking: Opportunities and risks. *International Review of Financial Analysis*, *81*, 102103. 10.1016/j.irfa.2022.102103

Ngai, E. W., Hu, Y., Wong, Y. H., Chen, Y., & Sun, X. (2011). The application of data mining techniques in financial fraud detection: A classification framework and an academic review of literature. *Decision support systems*, *50*(3), 559-569. 10.1016/j.dss.2010.08.006

Nelms, T. C., Maurer, B., Swartz, L., & Mainwaring, S. (2018). Social payments: Innovation, trust, Bitcoin, and the sharing economy. *Theory, Culture, and Society, 35*(3), 13-33. 10.1177/0263276417746466

Nicoletti, B. (2021). *Banking 5.0: How Fintech Will Change Traditional Banks in the 'New Normal' Post Pandemic*. Springer Nature. 10.1007/978-3-030-75871-4

Nikkel, B. (2020). Fintech forensics: Criminal investigation and digital evidence in financial technologies. *Forensic Science* International: Digital Investigation, 33, 200908. 10.1016/j.fsidi.2020.200908

Ojuwoni, A., Henry, A., & Oluokun, O. D. (2022). Evaluating Human Factors in Third-Party Services in Banking Sector. 10.31234/osf.io/pxv43

Ondrus, J., & Pigneur, Y. (2009). Near field communication: An assessment for future payment systems. *Information Systems and E-Business Management*, *7*, 347-361. 10.1007/s10257-008-0093-1

Panetta, I. C., Leo, S., & Delle Foglie, A. (2023). The development of digital payments–Past, present, and future–From the literature. *Research in International Business and Finance, 64*, 101855. 10.1016/j.ribaf.2022.101855

Parra Moyano, J., & Ross, O. (2017). KYC optimization using distributed ledger technology. *Business & Information Systems Engineering, 59*, 411-423. 10.1007/s12599-017-0504-2

Passi, L. F. (2018). An open banking ecosystem to survive the revised payment services directive: Connecting international banks and fintechs with the CBI globe platform. *Journal of Payments Strategy & Systems, 12*(4), 335-345. https://www.researchgate.net/publication/332568913_An_open_banking_ecosystem_to_survive_...

Puschmann, T. (2017). Fintech. *Business & Information Systems Engineering, 59*, 69-76. 10.1007/s12599-017-0464-6

PYMNTS. (2022, February 25). *Mollie Looks to Improve Marketplace Product With a Financial Services Suite for European SMBs*. Retrieved March 26, 2023, from https://www.pymnts.com/news/payment-methods/2022/mollie-looks-to-improve-marketplace-product-with-a-financial-services-suite-for-european-smbs/

Rajput, V. U. (2013). Research on know your customer (KYC). *International Journal of Scientific and Research Publications, 3*(7), 541-546. http://www.ijsrp.org/research-paper-0713.php?rp=P191526

Ramezani, J., & Camarinha-Matos, L. M. (2020). Approaches for resilience and antifragility in collaborative business ecosystems. *Technological Forecasting and Social Change, 151*, 119846. 10.1016/j.techfore.2019.119846

Rittenberg, L., Martens, F., & Committee of Sponsoring Organizations of the Treadway Commission. (2012). Enterprise risk management: understanding and communicating risk appetite. https://www.coso.org/Shared%20Documents/ERM-Understanding-and-Communicating-Risk-Appetite.pdf

Rong, K., Hu, G., Lin, Y., Shi, Y., & Guo, L. (2015). Understanding business ecosystem using a 6C framework in Internet-of-Things-based sectors. *International Journal of Production Economics, 159*, 41-55. 10.1016/j.ijpe.2014.09.003

Romānova, I., & Kudinska, M. (2016). Banking and fintech: A challenge or opportunity?. In *Contemporary issues in finance: Current challenges from across Europe* (Vol. 98, pp. 21-35). Emerald Group Publishing Limited. 10.1108/S1569-375920160000098002

Romānova, I., Grima, S., Spiteri, J., & Kudinska, M. (2018). The payment services Directive II and competitiveness: The perspective of European fintech companies. *European Research Studies*, *21*(2), 3-22. 10.35808/ersj/981

Scaringella, L., & Radziwon, A. (2018). Innovation, entrepreneurial, knowledge, and business ecosystems: Old wine in new bottles?. *Technological Forecasting and Social Change, 136*, 59-87. 10.1016/j.techfore.2017.09.023

Schlatt, V., Sedlmeir, J., Feulner, S., & Urbach, N. (2022). Designing a framework for digital KYC processes built on blockchain-based self-sovereign identity. *Information & Management, 59*(7), 103553. 10.1016/j.im.2021.103553

Schneider, M. (2023). Open Banking and Digital Ecosystems. *Digital Project Practice for New Work and Industry 4.0*, 169-178. 10.1201/9781003371397

Sebastian, I. M., Weill, P., & Woerner, S. L. (2020). Driving growth in digital ecosystems. *MIT Sloan Management Review*, *62*(1), 58-62. https://sloanreview.mit.edu/article/driving-growth-in-digital-ecosystems/

Sen, R., & Borle, S. (2015). Estimating the contextual risk of data breach: An empirical approach. *Journal of Management Information Systems, 32*(2), 314-341. 10.1080/07421222.2015.1063315

Senyo, P. K., Liu, K., & Effah, J. (2019). Digital business ecosystem: Literature review and a framework for future research. *International journal of information management, 47*, 52-64. 10.1016/j.ijinfomgt.2019.01.002

Shenton, A. K. (2004). Strategies for ensuring trustworthiness in qualitative research projects. *Education for information, 22*(2), 63-75. 10.3233/EFI-2004-22201

Skog, D. A., Wimelius, H., & Sandberg, J. (2018). Digital disruption. *Business & Information Systems Engineering, 60*, 431-437. 10.1007/s12599-018-0550-4

Soinski, D., & Theriault, M. (n.d.). The path to payment facilitation: Are you ready for the journey?. *J. P. Morgan*. Retrieved May 16, 2023, from https://www.jpmorgan.com/merchant-services/insights/pathtopayfac

Stake, R. E. (1995). *The art of case study research*. sage.

Steinert, M., & Williams, D. (2020). A KYC–AML utility: Driving scale, efficiency, and effectiveness. *McKinsey & Company*. https://www.mckinsey.com/industries/financial-services/our-insights/banking-matters/a-kyc-aml-utility-driving-scale-efficiency-and-effectiveness

Stripe. (n.d.). *Learn about payment methods*. Retrieved March 26, 2023, from https://stripe.com/docs/payments/payment-methods/overview

Subramaniam, M., Iyer, B., & Venkatraman, V. (2019). Competing in digital ecosystems. *Business Horizons, 62*(1), 83-94. 10.1016/j.bushor.2018.08.013

Sullivan, R. J. (2010, May). The Changing Nature of US Card Payment Fraud: Issues for Industry and Public Policy. In *WEIS*. https://www.researchgate.net/publication/46567288_The_changing_nature_of_US_card_payment_fraud_Industry_and_public_policy_options

Taherdoost, H. (2023). Blockchain: a catalyst in fintech future revolution. *Future Technology (FUTECH)*. 10.55670/fpll.futech.2.2.3

Takeda, A., & Ito, Y. (2021). A review of FinTech research. *International Journal of Technology Management, 86*(1), 67-88. 10.1504/IJTM.2021.115761

The Wolfsberg Group. (2018). *Mission – Global Banks: Global Standards*. Retrieved May 3, 2023, from https://www.wolfsberg-principles.com/about/mission

Tsujimoto, M., Kajikawa, Y., Tomita, J., & Matsumoto, Y. (2018). A review of the ecosystem concept—Towards coherent ecosystem design. *Technological forecasting and social change*, *136*, 49-58. 10.1016/j.techfore.2017.06.032

Visa. (2018). *Visa Payment Facilitator Model*. https://usa.visa.com/content/dam/VCOM/global/support-legal/documents/visa-payment-facilitator-model.pdf

Yadav, P., & Chandak, R. (2019, December). Transforming the know your customer (KYC) process using blockchain. In *2019 International Conference on Advances in Computing, Communication and Control (ICAC3)* (pp. 1-5). IEEE. 10.1109/ICAC347590.2019.9036811

Yao, M., Di, H., Zheng, X., & Xu, X. (2018). Impact of payment technology innovations on the traditional financial industry: A focus on China. *Technological Forecasting and Social Change, 135*, 199-207. 10.1016/j.techfore.2017.12.023

Yin, R. K. (2009). Case study research: Design and methods (4th Ed.). Thousand Oaks, CA: Sage. https://doi.org/10.33524/cjar.v14i1.73

Zahra, S. A., & Nambisan, S. (2012). Entrepreneurship and strategic thinking in business ecosystems. *Business horizons, 55*(3), 219-229. 10.1016/j.bushor.2011.12.004

Zetzsche, D. A., Arner, D. W., Buckley, R. P., & Kaiser-Yücel, A. (2020). Fintech toolkit: smart regulatory and market approaches to financial technology innovation. *University of Hong Kong Faculty of Law Research Paper*, (2020/027). 10.2139/ssrn.3598142

Appendix 1: Interview Guide

Introduction

1. Presentation of the author and academic background.
2. Presentation of the background and purpose of the study.
3. Clarification of how the interview data will be used.
4. Explanation of the interview structure.
5. Approval of recording the interview for analysis purposes.

Interview questions

Background of the interviewee

1. What is your role and function at [CASE COMPANY]?
2. In what way are/have you been involved in projects related to payment product distribution through third-party payment facilitators?

Payment product distribution through third-party payment facilitators

1. How do you perceive payment product distribution through third-parties?
2. What opportunities and long-term advantages do you believe payment product distribution through third parties create?
3. As a [ROLE TITLE], what do you perceive as the greatest challenges related to payment product distribution through third parties?
4. Why do you believe that these challenges occur and how could they be managed?

Considerations related to financial crime

1. As a [ROLE TITLE], what do you believe, in general, needs to be considered within [CASE COMPANY] related to financial crime risks?
2. From a financial crime perspective, what do you believe needs to be considered related to payment product distribution through third parties at [CASE COMPANY]?

Risk management

1. How do you believe that financial crime risks, in general, could be managed at [CASE COMPANY]?
2. How do you believe that financial crime risks related to payment product distribution through third parties at [CASE COMPANY] could be managed?
3. What role do you believe that risk appetite plays in regard to payment product distribution through third parties?
4. Do you believe that contracts could be set up with third parties to manage financial crime risks? In that case, what should the contracts include?

5. Do you believe that fraud monitoring programs could be implemented in relation to third-party payment product distribution? In that case, what could such a program look like?

Third-party payment facilitator perspective

1. Why do you believe that payment facilitators want to collaborate with [CASE COMPANY] through partnerships for payment product distribution?
2. What is your perception of how payment facilitators perceive their responsibilities in terms of managing financial crime risks?
3. How do you perceive payment facilitators' incentives to collaborate to manage financial crime risks?
4. How do you believe that payment facilitators perceive fraud monitoring programs with potential penalty fees?
5. Do you have any insights into how payment facilitators determine and use risk appetite concerning financial crime risks?

DEPARTMENT OF TECHNOLOGY MANAGEMENT AND ECONOMICS
DIVISION OF INNOVATION AND R&D MANAGEMENT
CHALMERS UNIVERSITY OF TECHNOLOGY
Gothenburg, Sweden
www.chalmers.se

CHALMERS
UNIVERSITY OF TECHNOLOGY