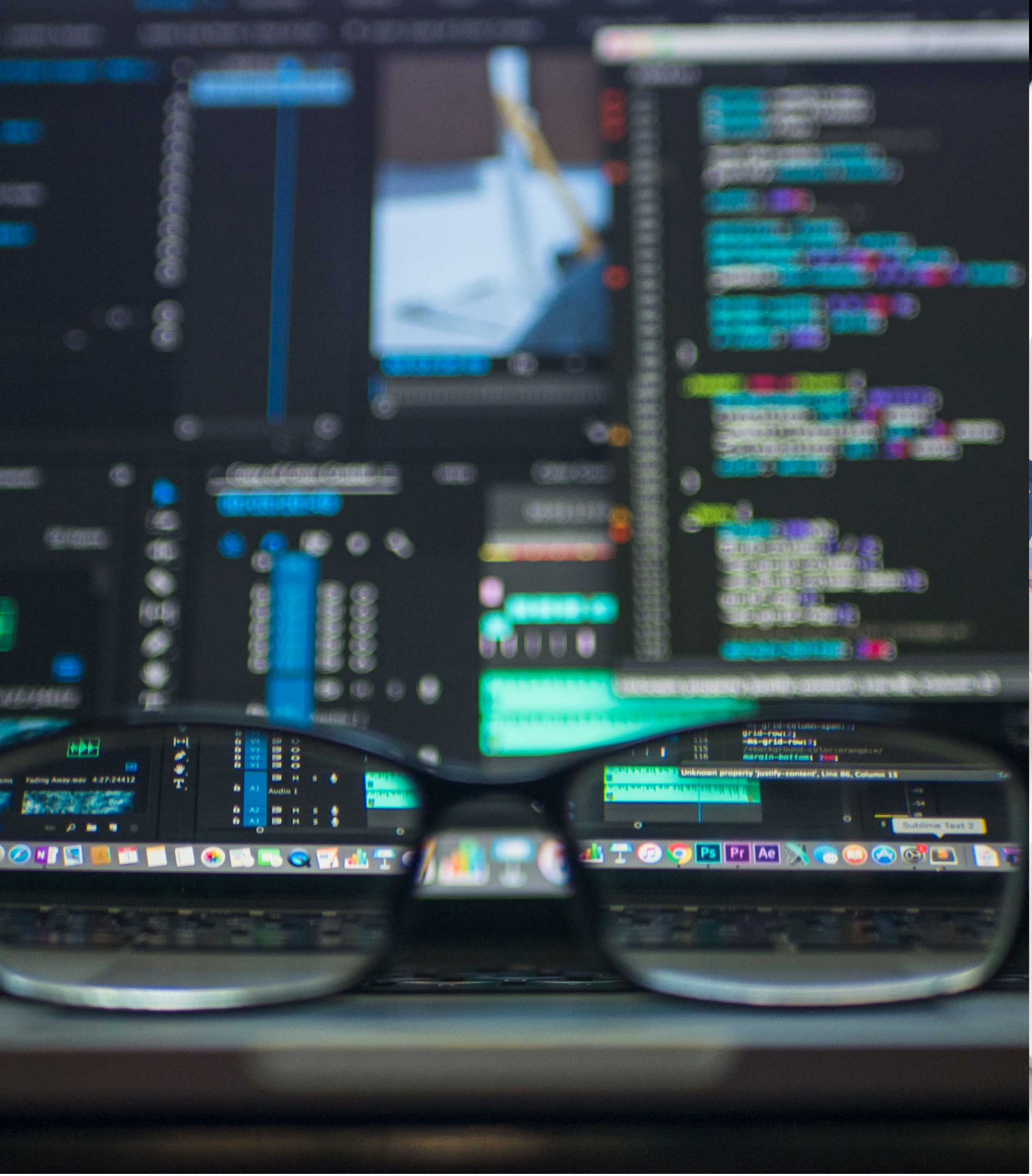


THE EMERGENCE OF NEW DATA ECOSYSTEMS IN FINANCIAL SERVICES
- RECENT DEVELOPMENTS IN SOUTH EAST ASIA -

Discussion Paper | September, 2021

Schweizerische Eidgenossenschaft
Confédération suisse
Confederazione Svizzera
Confederaziun svizra

Swiss Confederation

Federal Department of Economic Affairs,
Education and Research EAER
State Secretariat for Economic Affairs SECO

IFC International Finance Corporation
WORLD BANK GROUP

RIGHTS & PERMISSIONS

1818 H Street NW
Washington, DC 20433
Telephone: 202-473-1000
Internet: www.worldbank.org

This work is a product of the staff and external authors of the World Bank Group. The World Bank Group refers to the member institutions of the World Bank Group: The World Bank (International Bank for Reconstruction and Development); International Finance Corporation (IFC); and Multilateral Investment Guarantee Agency (MIGA), which are separate and distinct legal entities each organized under its respective Articles of Agreement. We encourage use for educational and noncommercial purposes.

The findings, interpretations, and conclusions expressed in this work do not necessarily reflect the views of the Directors or Executive Directors of the respective institutions of the World Bank Group or the governments they represent. The World Bank Group does not guarantee the accuracy of the data included in this work.

Rights and Permissions

ACKNOWLEDGMENTS

The publication of this study was made possible through the generous support of the Swiss State Secretariat for Economic Affairs. The study was conceptualized and led by a joint team from the International Finance Corporation's Financial Institutions Group and the Creating Markets Advisory teams, composed of Shalini Sankaranarayanan (Credit Infrastructure Specialist), Ivan Mortimer-Schutts (Senior Financial Sector Specialist), and Pratibha Chhabra (Credit Infrastructure Specialist), with support from within the World Bank Group under the guidance of Mahesh Uttamchandani and Martin Holtmann. The authors would like to acknowledge and express appreciation to the individuals and firms that contributed insights and information to this study, including Temasek Ventures, Alliance Bank, Estelle Darie-Rousseaux of AMRET, Andrea Baronchelli of ASPIRE, Axiata Group, William Lim of the Credit Bureau of Singapore, Michele Tucci of Credolab, CP Bank (Cambodia), Thomas Beurthey of Dibee, Mark MacKenzie of EFL Lenddo, FE Credit, Funding Societies, GrowSari, Nyha Shree, co-founder of Jumper.ai, the Indonesia Fintech Association, BG Mahesh of Sahamati, Felipe Valdes and Vince Parr of Tiaxa, Experian, TP Bank, Marie Steinthaler of Truelayer, Gianluca Pizzituti of Velotrade, Xero, Reddoorz, and Joachim C. Bartels, founder of the Business Information Industry Association. This publication also benefitted immensely from the participation, guidance, and insights of the peer reviewers and internal experts at the World Bank Group, including Margarete Biallas, Sören Heitmann, Collen Masunda, Matthew Saal, and Konstantinos Tsanis. The team would like to thank Charles Hagner for editing the report and Nitin Kapoor from Vertical Accord for designing the report.

TABLE OF CONTENTS

LIST OF FIGURES

ABBREVIATIONS

AML	anti-money laundering
CFT	combating the financing of terrorism
ERP	enterprise resource planning
KYC	know your customer
SME	small and medium-sized enterprise

50%
50%
50%
50%
№
NAME
BOSS
TOTAL
CATEGORY
1
2
3
4
5
Kovalenko
Lebedeva
Guraluk
Novak
Korkosh
Rogach D
Rogach D
Rogach D
Verenich I
Verenich I
100
98
98
350
140
ITME 1
ITME 2
ITME 3

CHAPTER 1

Executive Summary

Digital development has increased the array and availability of data relevant to making credit decisions. Banks rely significantly on information generated from existing client relationships, and on credit bureaus and registries to inform their credit decisions, but technology-driven innovation has spawned new types and sources of information and helped to capture existing data in machine-readable and digitally interoperable forms. Much of this is becoming available to financial institutions. Innovation has also ushered new actors into financial-services ecosystems, including new lenders as well as specialized firms that provide data collection, analysis, and intermediation services. From e-commerce and mobile telephone networks to point-of-sale, procurement, and accounting platforms, even smaller companies in developing markets are increasingly generating digital data trails that banks and other financial intermediaries can potentially use to improve credit scoring and enhance the means to assess and monitor credit risk.[1]

Historically, credit bureaus and registries have been the main pillars of credit information-sharing systems. While competing lenders have traditionally been united in their need for and willingness to share negative information (overdue, arrears, write-offs, and so on) on underlying borrowers, they have often been less willing to share positive information (for example, on-time payments, account balances, utilization rates, and so forth) for fear that their clients will be poached. However, given the benefits of positive information sharing, as evidenced through studies and the experiences of different markets, regulation is often put in place to mandate the sharing of credit information. Legal and operational standards and other best practices are often set to ensure consistency, security, and reliability. In addition, as credit information often touches upon sensitive, personal data, regulation often determines who can access such information, how it is to be handled, for what purposes it can be used, for how long it can be stored, and for how long consent to share data is valid or with what frequency such consent must be renewed.

The evolution of data ecosystems is testing the coherence and efficacy of policies and regulations that govern credit-information systems. With new data and new lenders on the market, who should be required to report or share data, and what scope of data should be subject to sharing requirements? Existing membership-based bureaus may not have appropriate incentives to expand access or data. New data intermediaries are complementing the role of central systems, and new lenders are complementing the role of banks, but these new players may not be subject to data-sharing regulations, raising questions about level playing fields. In some markets, through both legal changes and new business models, consumers are gaining more effective control over their own data, much of which is held with platforms, including banks. This prompts many to reconsider who should make decisions to share data and in what circumstances. Policy makers and industry participants recognize that innovation in the expanding data economy can have a positive effect on inclusion and efficiency, but there may be trade-offs to make with other primary policy aims, including protecting financial-sector stability, combating overindebtedness, and protecting consumer data rights and privacy.

This paper provides insights into recent business practices in Southeast Asia and market participants' views on policy and regulation issues. The research is based on a survey of data issuers, intermediaries, and users (primarily lenders). It focuses on understanding the role of new and alternative data and data providers in making decisions about credit. Some of these new forms of data—including social media data, cell phone data, and data generated from business processes, transactional data, online activity, and others—are being harnessed to support credit-granting decisions. Naturally, a greater number of players now collect, store, handle, and disseminate data relevant for credit-granting purposes, an area that was previously the purview of credit bureaus and credit registries.

Key conclusions from the research are the following:

(i) New data types and sources are rapidly becoming mainstreamed and hence are of growing importance to both new and incumbent financial intermediaries.

(ii) The market for credit information will continue to evolve, in particular with new analytics providers playing a role and with new data becoming available that is indicative of business performance.

(iii) There is a consensus among incumbents and new players that the current policy and regulatory framework for credit reporting will need to adjust to these new market circumstances.

But while most survey participants agreed that the status quo is not stable or efficient, and that there will need to be changes orchestrated or supported by policy makers, opinions diverged about what the focus of those changes should be. The main areas of concern for survey participants in the region were the following:

(iv) The playing field between incumbent credit-reporting institutions and new data-analytics providers should be leveled. Some parties believe that obligations to report data, access to such data, and standards of operation should be aligned and consistent.

(v) Some market participants were in favor of policy interventions to provide "public goods" that can reduce duplication of effort and enhance trust in new data and data models, such as through setting standards or audit requirements.

(vi) But others were inclined to support a more open and less regulated market, with fewer restrictions and regulations for all, including a reduction in constraints placed on existing credit-reporting infrastructures.

Chapter 2

Introduction

Data[2] has always been essential to finance, but today there is a lot more of it about. Few would dispute that new data can have value, and many would acknowledge that data is a fundamental component in the modern digital economy.[3] Data is increasingly seen not just as something to which access should be protected but also as a non-rival good that should be better mobilized in the interests of innovation, competitiveness, and efficiency, as well as to enhance financial-sector development and access to finance.[4] But fitting new types of data and new sources, providers, users, and supporting players into the existing structures for credit information is not as seamless as one could imagine. Credit-reporting systems require participating institutions to report specific data, but other lenders may not be part of these systems. New types of data that can inform lending decisions have become more readily available, but they may not be regulated as credit scores are; their providers may not be required to share it. Meanwhile, end users are increasingly provided with the legal and operational means to control and share data about themselves and their business with institutions of their choice, and in the absence of standards or third-party services, consumers of new data may duplicate each other's efforts to assess reliability and authenticity. In this context, policy makers and sector participants are reflecting on whether existing regulations and institutions are efficient and aligned with the emerging world of open data and "bigtechs." Should there be reforms to data rights and protections, standards, and infrastructures?

While the policy environment evolves on the ground, so does the market ecosystem. Many new data sources are quickly mobilized, working around the contours of the credit-information and financial markets to employ them wherever useful. The holders and generators of new and old data try to navigate changing rules for data protection and access. New companies offer businesses and consumers ways to use the data that they hold on, or generate through, other parties' platforms. Banks and other financial service providers are building more in-house expertise as well as relying on external data specialists to procure, analyze, and extract meaningful information out of new data. Meanwhile, financial institutions and credit-reporting organizations are still subject to regulations that do not apply to newcomers. Credit-reporting infrastructures are reflecting on their future role and implications for governance and regulation. The market is in flux, and policy measures need to deal with a moving target.

A diverse, new digital ecosystem has emerged and continues to evolve. Overlapping layers or waves of data-generating business service providers have emerged, building upon each other and transforming the former to create a distributed data ecosystem that rivals the role of existing bank-centric data ecosystems. These include the following:

(i) **Mobile operator and app-based data** on call and user behavior has been used by specialist analytics firms like Trusting Social, Tiaxa, and Lenddo to create scoring subsequently applied to products, including nano-credit and consumer and merchant credit.

(ii) A further layer of data has emerged from the growing usage of new e-commerce and platform-based **digital payments and merchant acceptance networks.** Services in the region, such as Alipay, Grab, Gopay, and VNPay, have generated new merchant data that has subsequently been used to assess the risk of short-term lending to them.

(iii) This has been complemented by more comprehensive **data about the business performance of consumers and merchants, captured on e-commerce platforms.** Consumer-facing companies such as Lazada, Shopee, and Tokopedia have leveraged data to support their own captive or arm's-length financing solutions with banks or person-to-person lenders and intermediaries.

(iv) A further layer of data providers has emerged as **business-to-business or "enterprisetech" service providers** offering inventory, sales, logistics, accounting, and customer relationship management platforms. Regional companies have been able to build on top of e-commerce, social media, and communication networks to provide simple cloud-based services that enable even sole traders to manage enterprise resource planning (ERP)–type data that can now also be accessed to support financial services. In more specific areas of business, such as energy distribution or agriculture, other more specialized enterprise data is becoming available and being used to support lending and other financial services.

(v) To help navigate this ecosystem and mobilize newly accessible data, more **specialized data analytics and intermediary financial services** have emerged. They are most clearly recognizable in "open banking" markets where they may be licensed as account information service providers and thereby have clearer rights to access and analyze data on customers' behalf, but even where there is no licensing requirement, these specialist firms exist. They alleviate the need for new data issuers to integrate in a bespoke manner directly with a multitude of lenders and financial institutions, and they provide expertise in data management and analytics that data providers may lack.

This expansion of the digital economy continues to add layers and sophistication to this evolving financial data ecosystem.

This study makes a small contribution to understanding the forces shaping this evolving market. The International Finance Corporation surveyed a cross-section of actors in this ecosystem to take stock of developments and generate insights for a broader discussion about the governance of credit infrastructure in a world of open data. The study seeks to understand the roles and views of new actors in the financial data ecosystem, the views of industry toward emerging policy issues, and the role that cooperation between such actors plays or may need to play in the credit-information industry. It also collected information about the operating models of selected firms, their range of services, and the legal and regulatory frameworks in which they operate, including how they handle consumer privacy and data protection.

The study gathered qualitative inputs from a cross-section of firms. Most are based and operating in Southeast Asia.[5] About 55 firms were identified and asked to participate; roughly half agreed to be interviewed. The firms were selected based on the aim of gathering inputs from the following three types of actors:

(i) **Data providers and issuers,** including financial service providers, government entities, utilities, and platform providers for business services, such as accounting, sales, and distribution

(ii) **Data intermediaries and service providers,** including credit bureaus, credit-scoring firms, and data-analytics companies[6]

(iii) **Users of data services,** primarily credit institutions and alternative lenders

Section 3 provides further details about the firms from which inputs were received.

A well-functioning data market is critical for financial institutions to make well-informed credit decisions. It is important that markets have efficient structures for exchanging data among lenders to guard against system-level risks, such as multiple borrowings and overindebtedness, which undermine the overall stability of the financial system.

Data has always been at the center of risk management and the "production" of financial services. Lenders in particular collect and manage data themselves to inform their credit decisions. They rely on various sources and service providers to access data about potential borrowers, and they often rely on market infrastructures, notably credit-reporting systems, to exchange data with other lenders about individuals' and firms' other liabilities in the market. Typically, data held in credit bureaus and credit registries includes (i) identification data, including name, address, and contact details; (ii) information about credit history, including but not limited to data on credits granted, outstanding balances, and repayment terms; (iii) repayment behavior, including on-time payments, minimum payments, late payments, and defaults; and (iv) other negative events, such as bankruptcies.

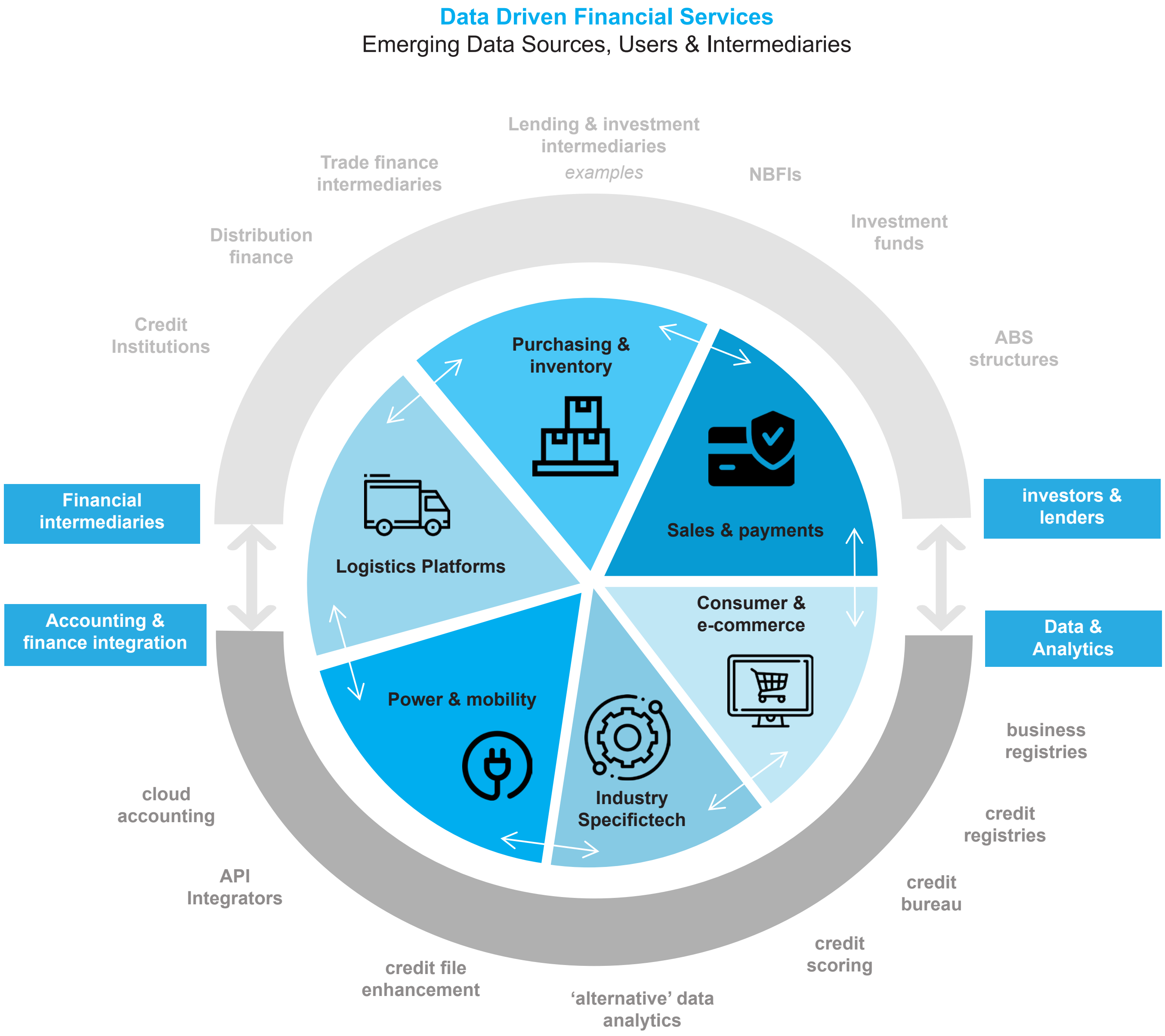


Figure 1: The Emerging Data Ecosystem

Access to data and verification of its accuracy or authenticity have always been challenging. Data has often not been machine readable; it has and continues to be stored in silos, in different formats, lacking standardization, and without adequate quality control or management measures. Traditionally underserved market segments, including small and medium-sized enterprises (SMEs), have generally had thin or no verifiable data records, especially in terms of those used most by credit institutions. For instance, they often lack audited financial statements, which in turn disqualifies them for most traditional lending, thereby further reducing their data footprint. SMEs and their existing creditors, where they do have data, may also be reluctant to share it.

Credit bureaus and registries emerged to fill a void in information for lending purposes. They have generally served as repositories to aggregate structured financial history and identification data and transform such data into information that financial institutions could read and interpret easily. Over time, credit bureaus in particular expanded to start collecting information from what was considered alternative or nontraditional data—mostly from utility providers, mobile service providers, and telecom operators. In Latin America, for instance, credit bureaus have long collected data from retailers offering goods on credit. The value of utilities data is gaining prominence as more bureaus around the world start to incorporate such data.

Digital transformation—of finance and also of other economic activities—is expanding the volume, granularity, and array of machine-readable data available about all types of entities, including SMEs. This includes financial as well as nonfinancial and behavioral information about a business's operations, the market in which it operates, and its suppliers, competitors, and clients. Data standards are evolving so that it is becoming easier to merge and compare data sets from different domains. Formerly off-line data has become online, and it is becoming increasingly available in near real time and accessible on an on-demand basis via application programming interfaces. This is particularly relevant for reducing information asymmetries and the costs of risk appraisals, potentially leading to enhanced access to affordable credit. Newly accessible data that is being considered and is accessible for credit underwriting includes social media data, cell phone data, data generated from business processes, transactional data, online activity, and others.

While data from credit bureaus and registries will continue to be critical, financial institutions are increasingly complementing it with new data. Bureaus and registries will continue to capture defaults and total exposure of borrowers, enabling lenders to assess the risk of overindebtedness/evergreening, but creditors are increasingly supplementing this data with other data. To help them access and make sense of new data, they are also often turning to new data-analytics firms and tools. So, in addition to the traditional credit-reporting service providers such as Experian, TransUnion, Equifax, and several others, lenders (both old and new) are either using or experimenting with their own data analytics to appraise, score, and make lending decisions or leveraging third-party analytics companies. Real-sector companies are also increasingly leveraging the power of their own data to offer financing solutions to clients that otherwise would not have access to finance or perhaps only at a higher cost.

New data and analytics can play an important role in boosting efficiency and expanding access to finance. This applies especially to traditionally underserved segments of the population, including women, micro, small, and medium enterprises, and the informal sector. While digital transformation is happening throughout the financial sector, new data and analytics can arguably have the biggest impact on parts of the economy that often suffer high barriers to entry and inefficiencies, in part due to the cost of assessing and monitoring risks relative to the potential to generate income for financial service providers.

The rise of new data sources makes new actors and stakeholders relevant in the broader financial data ecosystem. Alongside familiar and well-established actors in the credit ecosystem, such as financial institutions, credit bureaus, and registries, an array of new partners are of growing importance. This includes actors providing the new digital forms of core business services, such as for accounting, ERP, sales management, and payments. More sector-specific data types and providers, such as in logistics, distribution, trade platforms, even the tracking of agricultural inputs and production, are also of growing interest to financial institutions. (See figure 1)

The variety of institutions playing a role in originating loans or assessing and monitoring financial risks is also increasing. Access to new and alternative data sources is enabling new participants beyond established credit institutions to play a greater role in lending to SMEs. This includes specialized financial institutions (for example, in factoring or distribution finance companies), market-based investment vehicles, and real-sector firms that provide trade credit to clients and other business partners. However, not all of these institutions report their exposures to established credit-reporting systems. Often, they do not consult existing credit bureaus and/or registries as part of their risk-assessment processes.

The COVID-19 pandemic has enhanced the importance of these trends and issues. It has produced a negative economic shock, focusing credit institutions' attention on the preservation of portfolio quality, rather than on expansion. It has also driven far more economic and social activity online. It has restricted mobility and access to points of service such as bank branches or agents for topping up mobile credit and paying bills. The relevance of alternative data is hence growing, as lenders search for new insights to support lending decisions. This has led many financial institutions to accelerate their investments in digital operating models and data-driven services and analytics. Alternative data is increasingly being used—for instance, to detect and manage the incidence of fraud and to understand the ability to repay based on the pandemic's economic impacts on businesses by industry, sector, and so on. Alternative data is also enabling the provision of credit facilities to support working-capital needs, which are largely not met well by the traditional financial sector.

With this profusion of data, data sources, and new actors and business services, it is essential to take stock of market developments and ask whether the policy frameworks in which markets operate today are still fit for purpose. Broadly, there is a growing consensus that the answer to this question is no. Yet it is much less clear what the ideal new framework should look like, on what market and economic factors it may depend, and, not least, what policy actions and sequencing should be pursued to work with the market to move in an orderly manner from where we are today to a more appropriate structure in the future. Issues surrounding data cut across multiple interrelated policy domains, including opening banking or open-data regimes, competition policy, data market strategy, digital trade agreements, data protection and privacy and credit information sharing. These are briefly discussed in section 3.

The rest of this paper is structured as follows: Section 3 outlines the policy and economic context of this research and its relevance to ongoing reforms. Section 4 provides information about the design of the survey, including an overview of the survey structure, questions, and respondents. Section 5 reviews the findings and observations that emerged from the survey interviews. Section 6 briefly analyzes the findings and identifies the key emerging issues, which are then discussed in section 7 in the context of policy implications and avenues for further research. The conclusion summarizes implications for market stakeholders, including policy makers, development finance institutions, and industry bodies. Appendix A lists the companies that were covered by and/or participated in the survey.

binance.com
Hora 15m 1h 4h 1D 1S 1M
Original TradingView Profundidad
Spot
Límite
Comprar ETH
Vender ETH
Aislado 10x
Stop-Limit
Precio
Cantidad
1673.69 BUSD
Iniciar Sesión o Registrarse Ahora
Órdenes de mercado
Mis operaciones
Actividad del mercado
Fondos

Chapter 3

Policy Context

Several policy domains influence access to and usage of data for credit-underwriting decisions and managing credit risk. Most directly related to this study are the considerations for reforms to credit-reporting rules and regulations and principles for credit-reporting infrastructure. However, as the scope of information of relevance to credit-risk management and underwriting grows, so do the neighboring policy domains that shape (or in the future will shape) access to and usage of other data and information sources. (See figure 2.) These include both trade and competition policy, especially as they apply to data and digital services, the adjacent policy space of open banking, data privacy laws, and overarching strategies for supporting the data market and economy. The relevance of each for this survey and research is highlighted briefly below.

Open Banking & Finance

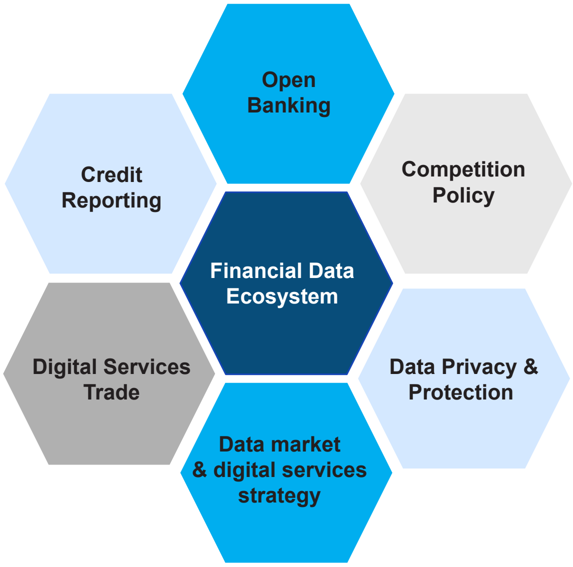
Data access regimes enabling clients to provide consent to third parties to access their bank account balance and transaction data; new providers using access to enhance or create "thicker" credit files.

Credit Reporting

Revising access and reporting rules to encompass the growing array of data services and lenders and align with the intent of General Principles

Competition Policy

Reviewing the market power of bigtechs and other holders of significant data; assessing the way they use this data and control access to compete in other fields including financial services; issue of reciprocal access being raised to create level playing field



Digital Services Trade

Agreements seeking expanded cross border access to public and private data sources such as registries, ID utilities Trade agreements to permit cross border transfer and processing of data

Data Privacy & Protection

Setting rules for actors across the economy, including the financial sector, on protection of and rights to consumer data

Data Market Strategy

Policy frameworks setting out strategy for development of data market structures needed to support new economy, including provisions on access, ownership, taxation

Policy domains shaping the evolution of financial data ecosystems

Figure 2: Policy Domains Shaping Financial Data Ecosystems

3.1 Credit Reporting

Credit-reporting systems are a critical part of financial market infrastructure. They coordinate the sharing between financial institutions of positive and negative credit data that can help to reduce system-level risk. As credit information is a non-rival good (for example, its use by one bank does not deprive another of its usage), clear economic benefits are generated by such systems. Their failure, or their absence, can undermine the stability of domestic financial systems, with implications for broader global financial markets. Robust credit-reporting systems can promote access to affordable and sustainable credit for individuals and companies and promote financial stability and economic growth.

Credit-reporting systems have primarily relied on structured, traditional credit data from licensed financial institutions and other regulated lenders. They have typically been categorized as credit bureaus and credit registries. The former support the credit-underwriting function of credit providers, while the latter typically serve to support the prudential supervision and systemic monitoring functions of financial market supervisors.

Information sharing is a business based on trust and transparency. A solid legal and regulatory framework is therefore a critical element to give both lenders and borrowers confidence about data processing and correct utilization. A monitored and regulated exchange of credit and other relevant data for permissible and limited utilization (for example, risk prediction, credit granting) can strengthen lenders' confidence in the system and better stimulate their participation.

The credit-reporting regulatory framework varies from country to country. In some cases, the laws governing credit reporting are part of a broader financial services law (for example, a banking law). In other countries, a separate, specific law on credit reporting has been passed (most countries in Europe and the Central Asia and Africa regions). In still others, a comprehensive data privacy law exists and also regulates—among all other data flows—credit information sharing (for example, all 27 European Union member countries). Finally, regulations issued by the banking regulator (that is, the central bank) often suffice to establish credit reporting (even private credit reporting and the establishment of private credit bureaus, as in the case of Egypt, Honduras, and Nicaragua). Occasionally, in some countries, sharing of information is not regulated but simply based on the borrowers' authorization (consent) to exchange and process data, generally supported by a code of conduct signed by the lenders and the private credit-reporting service provider.

A specific law on credit reporting is generally the most dependable, complete, and solid legal solution. However, any of the abovementioned regulatory approaches can enable the legal framework for credit reporting. Some of the core provisions covered in a robust legal framework include the following: (a) the role of the regulator; (b) entry and exit requirements in the form of licensing or registration; (c) permitted activities of the bureau; (d) data provider obligations, including obligations on data quality, accuracy, timeliness, frequency of updates, and others; (e) data user obligations, including usage where mandated, ensuring confidentiality and proper disposal of information; (f) permissible data and sensitive data that should not be collected or shared; (g) permissible purposes for the use of data, including limits on data access and use; (h) mandatory or voluntary sharing and inquiry; (i) borrowers' individual rights[7] to see, dispute, and correct their own data as well as procedures to enforce these rights (together with borrowers' consent, this is one of the most important guidelines of a modern, advanced legal framework for credit information sharing) and alternative dispute-resolution mechanisms; (j) the overall security of systems; (k) retention periods accounting for obsolescence of data (that is, how long information can be maintained in the database without penalizing borrowers and allowing them a second chance); (k) the ability to share or host data across borders; (k) violations and penalties in case of noncompliance; and (l) governance structures.

New participants in the credit-information space are often not subject to the same provisions that apply to the traditional participants. For instance, whereas traditional data providers (banks and other regulated lenders) may be mandated to share and/or inquire with a credit bureau,[8] alternative providers of credit (such as e-commerce providers, person-to-person lenders, and so forth) do not face similar requirements. In part, this stems from the fact that these entities were not (initially) regulated entities like traditional banks, and the traditional financial market regulators did not have the mandate to require them to participate in the credit-information system. This may be changing, however, as person-to-person lending crises have emerged, as in the case of China, pushing regulators to expand their regulatory ambit and require these alternative lenders (and, by default, data providers) to participate in a credit-information system. Figure 3 maps the key provisions applicable to participants in a traditional credit-information system and identifies whether new market entrants are subject to similar provisions (through other laws such as data-protection laws). The figure also shows where there appear to be gaps because participants are not subject to credit information-sharing laws or other governing laws contain no equivalent provisions.[9]

	Data intermediaries			Data Providers and Issuers			Data Users and Requesters	
Key provisions in credit information sharing frameworks	Incumbent credit reporting system & scoring providers	Data analytics service providers	New and 'alternative' data intermediaries & analytics providers	Established credit related data providers	New or potential 3rd party data providers	Public data sources	Established credit data users	Newer potential 3rd party data users
Regulatory Role	■			■			■	
Entry / Exit	■							
Permitted Activities	■							
Data Provider Obligations				■	■	■	▨	▨
User Obligations							■	■
Bank Secrecy	■			■			■	
Consumer Consent	■	■	■	■	■		■	■
Permissible Data	■			■				
Permissible Purpose	■						■	
Mandatory or Voluntary Inquiry/Sharing				■			■	
Consumer Rights / ADR	■			■			■	
Security and Systems	■	■	■	■	■	■	■	■
Data Retention Period	■			■			■	
Database Location	■	■	■					
Violations / Penalties	■			■	■		■	■
Governance	■							

Figure 3: Regulatory Provisions Applicable to Existing and New Credit-Information Stakeholders

General Principles for Credit Reporting [10] establishes five general principles for the development of credit information-sharing systems. The principles were developed to create a framework for the minimum conditions for the collection, storage, usage, and dissemination of relevant data for credit-underwriting processes. While the general principles defined two types of credit-reporting service providers based on the models that existed at the time, the principles themselves are meant to be entity agnostic, and the fundamentals of information sharing should apply across all entities that engage in information sharing for the purpose of enabling credit-underwriting processes.

At the time the general principles were established, there was a growing need to provide structure to a largely unregulated credit information-sharing market. As the information being dealt with was (and still is) sensitive and often personal customer data, it was important to set appropriate rules and guidelines pertaining to access and usage. Moreover, lenders often used the information exchanged through the credit information-sharing system to make critical decisions, such as whether to lend and, if so, at what costs and on what terms. The information accumulated through credit-information databases was also used for a variety of other purposes, such as enabling identification, preventing fraud, undertaking background checks in the context of employment applications, and so on.

Over the past several years, however, the credit information-sharing market has evolved, and new models and providers of credit information have emerged. In addition to the traditional credit bureau operators, several new players provide access to new forms of data or have the capabilities to assimilate and process new types of data for a variety of purposes, including for credit-underwriting processes. The general principles for credit reporting developed in 2011 were intended to provide guidance to the different stakeholders in the traditional credit-reporting space around data, data processing and security, governance, legal and regulatory frameworks, and cross-border data transfers. The principles also outlined the role of the different stakeholders and the oversight functions of the authorities responsible for supervising the credit information-sharing space. The principles were written with the relevance of data for credit-underwriting purposes in mind. In a sense, this limited the types of data that could be accessed and used specifically to make credit-related decisions. Further, the principles advocated for permissible purposes for credit information, to further control how credit information was used in different contexts. Since the general principles were established, several countries have opted to adhere to the principles while reforming or developing their credit-reporting systems. The principles are also used to benchmark existing practices in different jurisdictions.

Due to the expansion of data sources, types, providers, processors, and users, the principles may now warrant review to adapt to and reflect the changing market. The initial task force that wrote General Principles for Credit Reporting, now reconstituted as the International Committee on Credit Reporting, is also looking at the impact of the evolving credit information-sharing landscape and its implications for policy making, legal and regulatory frameworks, competition, consumers, and, subsequently, on the general principles themselves. In 2018, in partnership with the Global Partnership for Financial Inclusion, the International Committee on Credit Reporting laid out policies for the use of alternative data to enhance credit reporting.[11] These center around guidance on the use of alternative data; improving the availability and accuracy of information; expanding the remit of credit information sharing (through legislative reforms, increased oversight over the new types of credit-reporting service providers, and so forth); enabling cross-border flows of information balancing integrity, innovation, and competition; data privacy; cyber security; consumer protection; and pricing. While the basic tenets of the general principles continue to hold, the changing landscape and evolving policy considerations may require enhancements to the general principles to reflect the changing realities on the ground.

3.2 Open Banking, Finance, and Data

A central element of open banking[12] or open-data frameworks is to give users/clients of banks and other data producers more control over how and with what entities they, as data subjects, can share their financial data. Open banking in this sense is a sector-specific application of more general approaches to open data to give users more control over and access to their own digital records. An open-data framework may (i) recommend or define legal and technical standards and arrangements for clients to provide access to third parties, (ii) define the criteria that such third parties must fulfill to have access, (iii) state which data shall be made available, and (iv) specify whether data producers or holders must comply with such requests or whether arrangements are nonmandatory. The power of open-data frameworks is that it now unlocks access to previously siloed databases that were inaccessible because the holders of such databases restricted access to them. By giving control to the owners of the data—that is, the consumers themselves—open-data frameworks seek to overcome this challenge. While this approach begins to be applied in the banking sector, the application of open-data principles to other sectors is also progressing.

Different approaches are now being taken in different countries toward facilitating consent-based access not just to bank data but also to data from utilities or internet providers. In most cases, these forms of regulation will enhance access by third parties to data that can be used to supplement credit-risk profiling and assessments. In the European Economic Area, for instance, data-analytics and credit-scoring firms are already among those entities that have obtained the necessary licenses to operate under the applicable regulations as account information service providers. One of the unique benefits of open-banking services is the emergence and strengthening of alternative underwriting services due to access to such data. Many players around the world, such as Mint and Lending Club in the United States, are offering analytics services by leveraging open-banking systems. The traditional credit bureaus are also leveraging open-data applications to enhance their current offering. For instance, Experian Boost in the United States allows consumers to share details of their bill payments, including those for utilities, cable, and other services, with lenders or other users.

Next-generation approaches to more open and portable financial data are already emerging. Motivated by the same aims that drove the United Kingdom's Competition and Markets Authority to mandate open banking, the Bank of England has articulated the concept of an open-data platform that would enable a "portable credit file" that makes it easier for SMEs to apply for credit and improves transparency for lenders.[13] And in the broader context of decentralized data portability, several initiatives exist to develop and apply the concept of verifiable credentials[14] to financial and other services, so information that is on or accessible via the web can be issued and presented to potential "requesters" in a manner that is "verifiable." In financial services, this approach could widen the control that businesses and consumers have over their own data trails and address issues of trust when sharing such data—for instance, in the context of making a loan application.

3.3 Competition Policy

Control of customer data confers a competitive advantage; the emergence of data monopolies that could translate dominance in one customer segment to dominance in other areas raises concerns about competition and market access. Competition authorities are assessing the need for policy measures to enhance fair commercial access to, and consumer control over, data held by platforms, especially bigtech platforms with significant market power. Beyond considerations of breaking up some of the larger firms, there are questions about how to give users more control of their data, sometimes taking the same approach as that taken to open banking.[15] There are also concerns that some firms may struggle to get access to data on reasonable commercial terms. As more data is amassed on non-banking platforms, and as the size and market power of some of the platforms grow (for example, ERP or marketplaces), it is possible that competition-policy interventions could influence (i) the rights customers have to share that data with lenders or data-analytics firms, and (ii) the extent to which platforms can refuse or set onerous conditions for access to their data by other commercial firms.[16] Competition policy, therefore, is likely to have a significant impact on issues related to data access going forward.

3.4 Data Privacy

Data-protection and consumer privacy frameworks, long followed in European markets and most of Latin America, have been a critical part of the policy debate around data. The General Data Protection Regulation that came into effect in May 2018 was in essence a culmination of all those policy debates and discussions. It is widely seen as the standard for data protection globally, particularly in markets where no data-protection framework currently exists. The regulation protects people in the European Union from unlawful data collection or processing and works to increase consent requirements, provide enhanced user rights, and requires privacy policies that are written in an easy-to-understand way. Similarly, Asia-Pacific Economic Cooperation's Privacy Framework is a set of principles and implementation guidelines that were created to establish effective privacy protections that avoid barriers to information flows and ensure continued trade and economic growth in the forum's 27 countries. Unlike the General Data Protection Regulation, the framework is intended to provide a minimum level of protection, particularly in markets where no existing data-protection legislation exists. The objective of data-protection frameworks is ultimately to protect underlying consumers whose data is collected, treated, shared, or used for the development of various products and services. Credit-reporting service providers, as well as other data-processing entities, are required to abide by relevant data-protection laws, in addition to regulation specific to credit reporting in markets where such regulation exists.

3.5 Data Market Development

Policy makers are developing cross-sectoral approaches to data governance to promote innovation. Many governments are increasingly conscious of the potential of data-driven innovation to benefit citizens. Strategic plans encompass many initiatives, including efforts to enhance skills, support tech start-up communities, and improve the availability of government data. An important pillar of such strategies often centers on "data governance," with the intent to expand and improve interoperability and sharing of data. The European Union's data strategy, for instance, highlights "the need to support business-to-business data sharing, in particular addressing issues related to usage rights for co-generated data, typically laid down in private contracts." The approach taken by the strategy is to prioritize voluntary data sharing and to make data access and sharing compulsory only in specific circumstances. Overall, policy makers are taking steps to facilitate access to data and strengthening users' rights over the data they create (or co-create) in a manner that is likely to be of growing relevance to credit-reporting systems and their stakeholders.

3.6 Digital Trade

Trade agreements are increasingly integrating provisions on promoting cross-border data access and transfers. Digital trade is expanding worldwide, sometimes in stand-alone services but often also as complements to trade in goods and non-digital services. These flows may involve consumers, firms, or governments. It is important for data to be able to flow freely yet in a manner that is consistent with both domestic regulation and international trade agreements. A trade transaction itself may require access to and processing of data to verify counterparts' identities and fulfill commercial and regulatory requirements; financing, payment processing, or insurance for a transaction may require additional data that enables risk assessment and for risk to be monitored through the life cycle of the transaction. The data generated by (or that reflects) the track records of commercial parties' interactions can be of help in continuing to build and enhance a credit file in the future. New service providers, such as some of the fintechs and data-analytics providers licensed as account information service providers,[17] may seek to work across borders to collect, access, or process this information as part of risk-analytics services for lenders. In all these example contexts, it may be advantageous or even necessary to operate on a cross-border basis. Recognizing that credit-relevant data is produced by a range of nonfinancial multinational businesses means that credit data is already being produced, used, and stored across borders.

New trade agreements are emphasizing the need to create compatible regimes for data protection and to facilitate data transfers for the legitimate conduct of business. Some agreements, such as the Digital Economy Partnership Agreement between Chile, New Zealand, and Singapore, underline common ambitions to support data-driven innovation, particularly around digital services including fintech, and they acknowledge the need to enhance access to "public" data and to collaborate on data sharing more broadly to promote innovation. The European Union's recent trade policy statement singles out the issue of the digital economy and notes that "the Commission will work towards ensuring that its businesses can benefit from the international free flow of data in full compliance with EU data protection rules and other public policy objectives."[18] Similarly, in the United Kingdom's approach to trade negotiations with Japan, the facilitation of trade in or transfers of financial data was also noted as an objective. Also, the

World Economic Forum, through its Shaping the Future of Trade and Global Economic Interdependence Platform, promotes the interoperability for global data flows, including through trade frameworks and regulatory cooperation. While these new high-level agreements do not explicitly address access to credit-reporting systems or alternative scoring platforms, existing issues related to cross-border access to and regulation of credit information are likely to gain more prominence in the near future as negotiations on implementing measures progress.

As cross-border digital business expands, companies may need to comply with a growing variety of sometimes-incompatible regulations. Each jurisdiction may have different data-protection policies and rules and may require foreign firms to comply with them if the firms want to trade with (or within) those jurisdictions. This can lead to market fragmentation and increase the costs and complications of meeting multiple requirements, weighing often most heavily on smaller markets. It can also lead to extraterritorial application of requirements, as companies based in third countries may also find themselves needing to comply with foreign laws to indirectly meet compliance needs of partner firms. This is often mentioned in the case of EU or US laws and their implications abroad. In the absence of global standards, companies may find it more convenient to adopt the standards of larger and/or more internationally oriented jurisdictions, such as China, the European Union, India, and the United States.

Chapter 4

Research Approach

The research is based on interviews with a cross-section of firms active in providing or using alternative data for financial services. A questionnaire was used to guide the interviews. This was developed using the general principles for credit reporting as an initial framework. The research focused on understanding the differences between traditional credit-reporting service providers and other entities that now engage in similar functions.

Figure 4: Overview of the Survey Population Structure

	Function and No. of Respondents			Institutional Classification	Definition and Examples
(1)	Data intermediaries and service providers	5	a	Incumbent credit-reporting systems and scoring providers	Mostly regulated credit bureaus
			b	Data-analytics service providers	Including firms that source and provide bespoke analytical services but not proprietary scoring
			c	New and alternative data intermediaries and analytics providers	Firms providing data analytics and scores using non-bank or alternative data such as from social media, mobile usage, and so on
(2)	Data providers and issuers	9	a	Established credit-related data providers	Parties including banks and members of credit bureaus, such as utilities or government agencies
			b	New or potential third-party data providers	Originators or managers of new or potential data, such as social media, mobile network operators, and trade or e-commerce platforms, or cloud-based sales, ERP, or accounting systems
			c	Public data sources	Including property, company registration, personal ID, and other public databases
(3)	Data users and requesters	11	a	Established credit data users	Banks and consumer credit institutions
			b	New or potential third-party data user	Embedded finance players such as real-sector firms extending credit lines to clients

The main inputs came from 25 firms that responded via a written survey and online interview. An initial long list of 55 firms was established, composed of a balance of companies operating across the three functional roles identified in figure 4. The long list contained 12 data intermediaries, such as credit bureaus (of which five responded), 21 data issuers (of which nine responded), and 22 data users (of which 11 responded). In total, 25 firms participated in the survey. A further six stakeholders, firms, and experts, many with no direct commercial role, notably from the Business Information Industry Association and the Indonesia Fintech Association, also provided partial inputs and comments. The constituents in this overall long list were chosen based on knowledge of actors in the market.

It was not possible to create a randomized sample of firms. Precisely because this is a market in flux, there is no recognized list or registry of firms that fits this evolving space and from which a randomized sample could have been made. Only firms with operations in one or more Southeast Asian markets were chosen. (See appendix A for details.) The selected firms included existing investee clients of the International Finance Corporation and represented a mix of well-established and new firms operating in this area of credit data and analytics. The questionnaire was provided in writing to all interviewees. (See appendix D.) Most companies responded through both a live interview and written answers. The interviews were conducted between June and August 2020.

The reasons some firms declined to respond to the survey also provide valuable insights. Several firms, especially among the new potential data providers, indicated that they were interested in the topic but were still “unqualified” to answer. They indicated that they were just trying to navigate the market and regulatory issues that would influence their strategy for mobilizing data for finance. Other firms declined either because they were reluctant to share information about strategic projects that could have implications for their relationship with regulators, or because internal rules restricted their ability to share. This was the case mostly for firms that were not only mobilizing new data but considering how to play a more active role in lending operations. A few firms, especially large conglomerates, declined because they could not identify the appropriate department or function with authorization to address what they saw as still emerging, cross-cutting, and potentially sensitive legal issues.

Regulators were not included as part of the survey, as the focus was on understanding the market and industry perspectives on the topic. However, we note that findings from the survey point toward a need for greater legal and regulatory clarity. Consequently, we have added a brief high-level analysis of the legal and regulatory frameworks in the surveyed markets, based on desk research, as well as considerations that policy makers and regulators may want to keep in mind as they determine how best to regulate this space.

The survey focused in particular on firms with relevance to finance for SMEs and sole traders. Although it did not disregard other related issues specific to listed companies or consumer finance, the scope of questions and issues focused on understanding the role of data of most relevance to financial and credit decisions for SMEs and sole traders, as well as informal businesses. (See figure 5.) Data and services available about publicly listed companies and larger international firms may differ considerably from the kinds of data that are relevant to and available about SMEs.

Selected data types and coverage

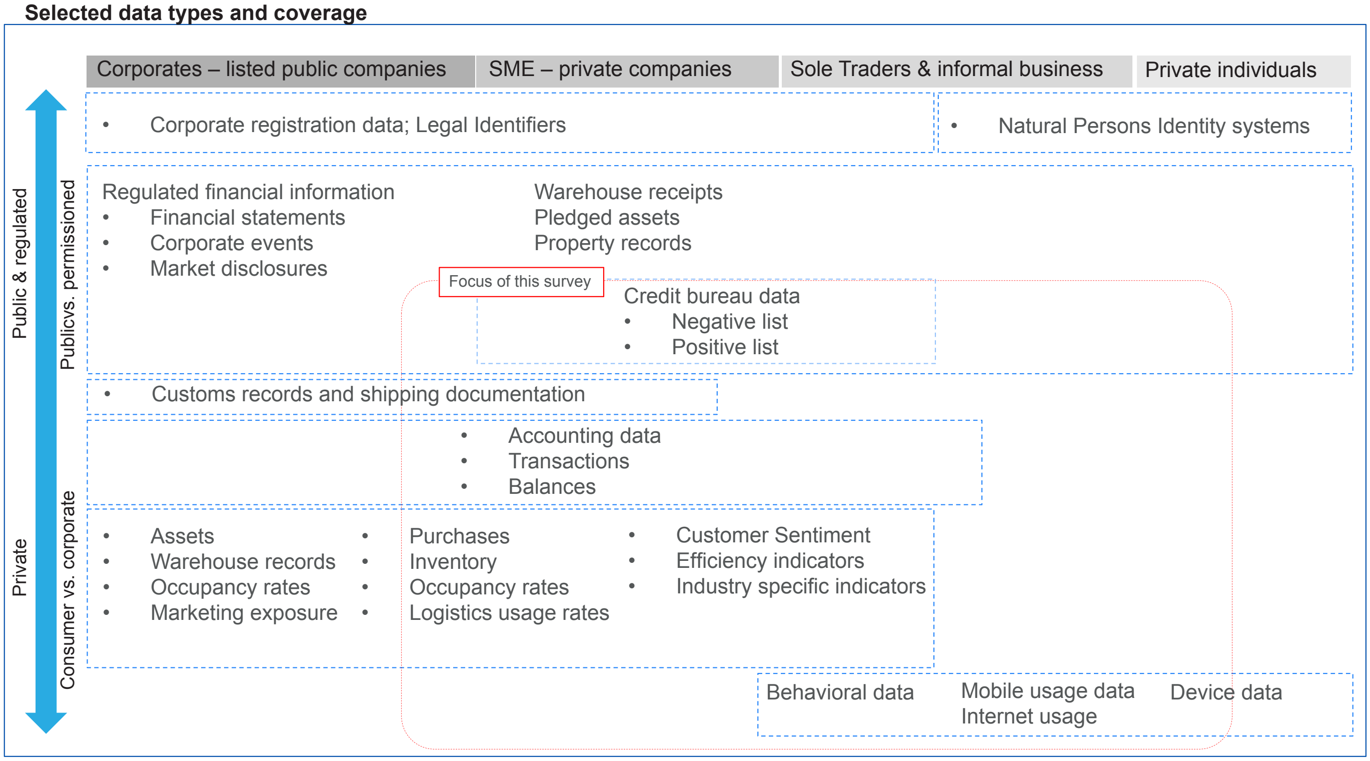


Figure 5: The Scope of Data Considered

In terms of policy questions, the survey focused on the following two topics:

(i) The framework of legal and regulatory requirements under which the surveyed firms operate

(ii) The interaction between business-model choices and regulation of credit information and analytics

The continued digital transformation and evolution of markets in Southeast Asia make this research particularly relevant. All the markets covered by the surveyed companies have one or more credit bureaus that are governed by specific credit bureau laws. Over the past decade, however, new digital businesses have created successive layers of data that have in turn been used by financial-sector innovators to develop scoring and support financial services, especially lending operations, for clients with a thin or no file or for small-scale business needs.

12:44
BTC / USDT
37 126,65
37 126,65 $ +3,55 %
High
38 708,27
Low
35 657,69
Vol(BTC)
91 526,80
Vol(USDT)
3 411 813 303,69
Line 15m 1h 4h 1d More Depth
MA(7):37 595,02 MA(25):37 144,45 MA(99):34 954,87
38 708,27
39 000,00
38 000,00
37 126,65
36 000,00
35 000,00
34 000,00
VOL:3 660,43
8 988,70
02-02 02-03 02-04 02-05
MA EMA BOLL VOL MACD KDJ RSI
Order Book Market History Info
Bid Ask 0.01
1,699586 37 126,66 37 126,67 0,015881
0,046587 37 126,65 37 126,69 0,017371
0,007452 37 125,61 37 129,06 0,141057
Currency Alert Buy Sell

Chapter 5

Findings and Analysis

The survey enabled firms active in the market to share their observations, views, and insights. Unless explicitly noted, summaries presented here represent views expressed by the surveyed companies.

5.1 Business Models

The business models of firms that are generating new data sources and providing new analytics in the region are still evolving. Parties to the research offered the following perspectives based on different models and approaches, especially in relation to credit processes:

(a) The survey covered an array of firms offering nonfinancial services—for instance, operating **e-commerce or enterprisetech platforms**. These firms are potential data issuers. They collect, manage, or generate data about their users that can reflect their financial needs and characteristics or provide indications of their business performance. These firm recognize the potential application that such data can have in financial services. Some have begun to develop their own internal financial service functions themselves; others are providing financial service providers with access to relevant data in their role as a distributor of financial services; while others enable their clients to leverage their own data but do not play a direct role in its commercialization.

(b) **Data-analytics companies** source data and provide risk management and analytics, including credit scores, as a service to users, primarily financial institutions. Some of these companies have a very narrow and specialized business model in which they only provide analytics, but other firms, to commercialize their skills, have also started to intermediate loans or make loans themselves based on their scoring expertise.

(c) **Incumbent credit bureaus** are developing their expertise in leveraging new data sources and in developing new products, such as credit scores, to complement existing data-collection and reporting services, either by developing internal capacity or by partnering with other data-analytics companies that are more specialized in developing these types of products and services.

All the surveyed firms view new data-analytics and risk-management products broadly as complementary to the services of existing credit-information service providers, but some respondents implied that if performance data (for example, sales and income indicators) were to become very reliable and comprehensive, this might substitute for traditional credit checks and compete with existing scoring services. The new data-analytics companies largely viewed themselves (and were also viewed by their users) as providing information relevant to no-file or thin-file customers that do not hold traditional bank accounts, or that are thinly served by traditional financial institutions. Hence these companies fill a void in the market by addressing the information gaps of those that have historically been unserved or underserved. The market view was that if third-party data-analytics companies were to handle loan performance data, it would be appropriate to apply rules to them that apply to the equivalent activity of credit bureaus.

5.2 Data Types and Data Quality

In all markets, credit bureaus continue to be the only repositories of traditional financial-history information about clients of regulated lenders. Banks and other regulated lenders continue to rely on credit-bureau information, where available, before turning to other sources to supplement their data needs for credit underwriting. Where they said they do use alternative data, through data-analytics companies, surveyed financial institutions indicated that they struggled initially to understand the underlying data used in alternative scoring models as well as its quality, although this has improved over time.

All survey participants are actively collecting, managing, and using data from a variety of conventional and unconventional sources. Alongside banks and credit bureaus, the survey solicited inputs from firms providing or managing data from point-of-sale systems, payments, mobile telecoms (including messaging, talk, data, and payment for these services), mobile device data, accounting platforms, e-commerce sales, and logistics. In many cases, it is important to note that data used for both marketing and risk purposes derives from the actual interactions or transactions conducted between customers/users on a given platform for payments, commerce or social media, and so on. In one case, transaction data was complemented with the tracking of stock in and out of warehouses. It was noted that accounting-solution providers can be important not just to gain access to financial accounts but also to help verify or cross-check the accuracy of data obtained from other platforms on sales figures or procurement expenses. By looking, for instance, at cash flows, invoices issued, and receipts, and reconciling this information with bank statements, or by looking at a customer's tax-payment history (where available), they can further attest to the validity of the data. This observation by the respondents highlighted the importance of interoperability, so that different data sets can be "merged."

Some firms have used social media, location, and network data, including behavioral data, for scoring purposes. A number of users, including banks, fintechs, payment service providers, e-commerce providers, and insurance companies, increasingly use telco data to help detect fraud or conduct know-your-customer (KYC) checks. Behavioral data, which can include records of app usage or consumer interactions with devices, enables data users to determine fundamental borrower traits with implications for creditworthiness. Some analytics firms expressed interest in, or positive views of, the potential to integrate industry-specific production or distribution data as part of their risk-scoring and management analytics. Government data was also noted as important, especially to support anti-fraud controls and compliance with identity checks—anti-money-laundering (AML) and KYC—but not all providers had ready access to government-led or public databases.

Not all data is viewed or treated equally. Within the ecosystem of data-analytics providers, there is generally an acceptance that banking data has the most weight and relevance when it comes to assisting in the credit process. The data from banks holds greater value because it is systematically captured in a consistent, reliable, and machine-readable fashion over long periods of time. In addition to the actual data itself, the accuracy, consistency, periodicity, and depth of data are all important characteristics that add to its value. Data-analytics companies are leveraging alternative data streams to provide innovative ways of assessing customers' overall financial health that are particularly relevant for onboarding thin-file customers. While these new forms of data can be useful for the financial sector, such data should be evaluated as banking data is—for accuracy, consistency, periodicity, and depth, as well as veracity—to ensure that meaningful insights are derived that minimize risks and harm to the underlying customers. Accounting data, for instance, is only as reliable as the inputs provided by the underlying customer. Without robust audit controls, its value is questionable. Further, scope matters: Accounting solution providers with broader market coverage can enhance the utility of their data pools by analyzing metadata. The more widely their solution is adopted in the market, the more likely they are to have cross-sector comparisons that supplement firm-level insights.

Credit bureaus typically serve the data providers that share data with them, as most information-sharing agreements are based on "reciprocity principles." Reciprocity is key to ensuring the integrity of data in the system, as data providers are more willing to share their data if they are assured that they will also see equivalent data from their peers. Moreover, it ensures fairness, in that data users can access and view data only if they are willing to share their own data. Reciprocity rules therefore generally apply to all participants in credit bureaus, including banks, non-banks, microfinance institutions, utilities, telcos, and so forth. Third-party data-analytics providers, on the other hand, do not operate on the basis of reciprocity principles. They access data as needed to support their clients' portfolios (traditional and nontraditional lenders and non-lenders, including banks, fintechs, neo banks, rental companies, and so on) and often for a price. This can have limitations in terms of accessing certain data, viewing complete data, or cherry-picking data depending on costs or the mandate/need of the client.

5.3 Legal and Regulatory Frameworks in Survey Countries

While credit bureaus are licensed and regulated in most of the survey countries, companies that provide innovative scoring solutions using alternative data are generally not covered under credit-reporting legislation. Of the countries covered by the surveyed companies, only Indonesia was noted as having created a specific regulation governing the activities of these entities, under an all-encompassing digital innovation regulation meant to capture a wide range of innovative financial technology business models. [19] As part of the regulation, these entities are required to record themselves with the financial services authority, participate in a regulatory sandbox, and then, if approved by the regulator, proceed to obtain registration. The regulation stipulates that these providers self-monitor; submit periodic reports to the regulator, including a self-assessed risk report; operate within the country; comply with personal-data-protection, AML, combating the financing of terrorism (CFT), and consumer-protection laws and regulations; and provide consumers with information regarding the status of their applications—and reasons thereof. In addition, these companies are also subject to the Electronic Information and Transaction Act[20] and limited liability company laws.[21] Survey participants operating in Indonesia provided mixed feedback, however, on whether the existing legal and regulatory framework and its enforcement was clear enough; some participants indicated that more clarity was required for companies engaged in alternative scoring solutions, including clarity on the use of alternative data.

Generally, it was found that companies providing data-analytics services are bound by and comply with personal-data-protection and privacy laws applicable in the jurisdictions in which they operate. There are no specific regulations around the provision of data-analytics services or alternative credit scoring. The regulatory framework for such companies is also potentially dependent on the data and business operations model; if the companies are assessing financial data (in partnership with lenders), their alignment with requirements that are applied to them and to credit bureaus, and the consistency with which the requirements are applied, may need to be reviewed. Where these companies provide e-KYC services, they have specific approval for it from the financial services authorities and work under the ambit of overall AML/CFT regulation of that particular jurisdiction.

Beyond data-protection and privacy legislation, most respondents consider the structure and scope of regulation to be very unclear. Especially among new data-analytics providers, there was a sense that an absence of clear regulation did not necessarily mean that they were not subject to legal risks. Companies said that a lack of specific regulation, while in principle leaving them with more commercial freedom, creates uncertainty and does little to support trust in new services. This is perceived on balance to curtail the development of new data-analytics providers and related capabilities. Also expressed was the further concern that, where laws exist, they are often articulated as very high-level principles and lack implementation detail. This creates additional uncertainty among institutions about how to comply and risks introducing heterogeneous interpretations.

5.4 Data-Analytics Governance/Oversight

There were few examples of advanced or specific regulation or oversight of data-analytics providers or services. Within the group of surveyed firms, lenders are seen in practice to be (even if not), and actually are formally, at least via outsourcing regulations, responsible for the quality and integrity of the alternative scoring models that they may use (whether developed in house or outsourced). While in some countries, credit scoring and rating are regulated, the provision of scoring models may not be. As a core function of the bank, the use of alternative data and models, if outsourced, will be considered material. For instance, under guidance from the European Banking Authority, banks should retain the ability to reintegrate these functions and the ability to identify, monitor, and manage risks. Lenders using or considering the use of new analytics and data voiced concerns about how scoring models are developed (for example, about inputs, assumptions, and outputs) and noted that a lack of maturity, track record, or regulation was a disincentive to their uptake and use. Analytics providers indicated that, while they may not be subject to an external audit of their models, in some cases they would be reviewed by the risk departments of banks that employ their models. In some cases, they also work with the regulators to explain their process, and in some markets, the models had to be approved by the regulator. Some of the analytics providers mentioned having in-house data and model governance frameworks in place to ensure that they would be compliant with any future regulatory mandate. Apart from the application of outsourcing regulation to banks, there was no notable consistency across markets and players with regard to the role of regulators in such assessments.

Some firms suggested that regulators themselves face challenges in assessing new models. They do not necessarily have the appropriate staff or the skills needed to understand the underlying data sets and modeling techniques. It was further seen as being difficult to regulate this activity, given the lack of homogeneity in the alternative data market.

Some firms suggested that the presence of a few vendors that sell different risk models based on "bad science" undermines the market. The risk liability, however, lies entirely on financial institutions. One of the surveyed financial institutions said that model outputs developed by different providers varied and that they had to work with different players to agree on a minimum standard of quality that would be acceptable to the institution. That entity expressed the opinion that there would need to be some form of risk sharing in the industry eventually, [22] since financial institutions are currently taking on the risk entirely of using model outputs in their credit decision-making processes.

From a financial institution's standpoint, it would be helpful to be able to rely on external means to verify or establish a degree of comfort with these models. This would help to minimize the institution's own liabilities and make using new data sources and models more attractive. Data-analytics providers, for their part, would benefit from developing industry codes of conduct and self-governing in the absence of any legal and regulatory oversight.

5.5 Consent and Privacy

The data privacy–related practices of analytics companies may require further evaluation. Third-party data-analytics providers rely on their clients (mostly banks and financial institutions) to fulfill obligations to the end clients (for example, borrowers), such as respecting client confidentiality, obtaining consent, maintaining proof of having acquired consent, retaining consent, and so forth. In the case of companies that leverage social media platforms such as Facebook and WhatsApp, it was noted that the data-privacy policies of these platforms also apply to the third-party analytics providers. None of the companies interviewed had a process for explaining to underlying customers (who were being scored) how results were obtained. The third-party analytics companies, for the most part, rely on their clients (for example, the lenders) to handle all interactions with the customers and depended on them to explain or not explain the underlying scoring rationale.

Nearly all surveyed companies indicated explicitly that they obtain consent from users when information is collected, processed, or shared. Often contracts, terms, and conditions include an opt-in consent clause for specific, permissible, data-sharing purposes. Third-party data-analytics companies and providers of services rely on their clients to acquire the consent of data subjects, similar to traditional credit bureaus. If the clients are regulated entities (like financial institutions), then they are in turn responsible to their supervisory bodies for reporting on consent practices and ensuring compliance with relevant legislation. However, for clients that are not regulated (for example, users of accounting solutions or merchants on e-commerce platforms), it is unclear what kind of external oversight mechanism exists to ensure that these clients are in compliance with consent requirements in each jurisdiction. Some surveyed companies indicated that they collected consent for each use of data, implying greater awareness for the underlying consumers. But some survey participants expressed concerns about the use of alternative customer data even with consent, as what could appear to be harmless variables could lead to behavioral profiling and the redlining of customers.

Issues of consent that arise in the context of traditional financial service providers and bureaus also apply to the new data-analytics providers. Some these key challenges are the following: (a) Consent clauses are often embedded within “pages and pages of text” on privacy policies, which borrowers may not read fully or understand; (b) acceptance of the terms and conditions regarding privacy policies are required prior to being able to use an app or access the services offered by a company; (c) consumers do not often withhold consent when they are in need of a credit product or any other product; and (d) the language used in privacy policies is often lengthy and complicated and may not be appropriate when addressing borrowers at the lower end of the financial services pyramid.

It was not clear what legal and practical means are available to consumers to check and validate the accuracy of their own information handled and treated by third-party data-analytics companies. Unlike credit bureaus, most of these entities do not have consumer-facing portals and cater only to the needs of their members/users. Consumers don’t have rights of access to the information about them that companies hold, process, or treat and, hence, no means to check the authenticity of their own data or records of which institutions had accessed it.

5.6 Security and Data Protection

Most of the companies indicated that they are bound by data-protection legislation, at least in markets where it exists. If they processed data related to entities in the European Union, they followed the rules of the General Data Protection Regulation. Some firms noted that, where possible, they applied principles of the regulation even outside the European Union, to adhere to what they currently see as the highest standard in this space and to simplify processes. While several countries have broad consumer and data-protection rules or principles, these were often seen as not particularly adapted to the credit data business.

The surveyed companies generally indicated that they had appropriate security infrastructure, systems, and processes in place to ensure data security. In terms of the data security, the respondents confirmed that data anonymization, multitiered encryption, security certificates, and relevant disclosures to customers were the key measures taken to ensure security. Respondents also follow industry standards in terms of ensuring security of IT infrastructures (ISO 27001) and data centers, with multiple layers of security, such as two-step authentication.

None of the new data-analytics providers said a specific supervisor oversaw them for issues of security and data protection. Surveyed companies were not subject to third-party assessment or checks of their IT security systems and processes, nor did they mention any supervisory checks of the same.

5.7 Compliance

All financial service providers and most analytics companies have a dedicated compliance function, but some nonfinancial companies manage compliance issues in combination with their broader legal affairs. Traditional data providers, particularly regulated financial institutions, and credit bureaus have a dedicated internal compliance function to ensure compliance with relevant laws and regulations. For those with a dedicated team, the actual size and scope of these teams varied depending on the size of the entity. The new entrants in the data-analytics and alternative-scoring markets rely largely on their clients (regulated financial institutions/lenders) to comply with relevant laws and regulations, such as meeting consent requirements, data privacy obligations, and conducting KYC or AML checks, so that any data they access, treat, handle, or use for developing analytics and scores would be considered compliant by default. Some of the smaller companies said they rely on external counsel, often kept on retainer to provide guidance relevant to the specific local jurisdictions in which they operate.

5.8 Cross-Border Information Sharing

Cross-border information sharing was not yet seen as a critical issue or constraint.[23] Firms across the surveyed population were focused largely on serving local markets, using local data for local commercial and financing needs. Where a company indicated that it had a presence in multiple markets, it said it follows local regulations, such as for data residency. The eventual need or ambition to scale across borders was raised, but only a few surveyed companies are engaged in cross-border trade in real-sector or financial services. Hence, with limited exceptions, the survey indicated that the need to access data sources in another jurisdiction and to transfer data across borders was not yet acute. The main exception to this was a general concern about the ability to store and process data in the cloud through international as well as domestic arrangements. The need for common governance standards, however, is recognized, and parties are beginning to discuss it. [24]

5.9 Ecosystem Integration and Partnership Development

Many of the companies categorized as data providers or issuers indicated that, while they hold data and see value in data, they are still exploring the best ways to maximize the usage of it. Given that the survey explicitly targeted new and potential data providers, this may not be surprising, but there was some expectation during the design phase of the survey that the selected companies would have clearer strategies for data, even if they were still at early stage of implementing them. The input from the survey suggests that a lack of clarity not just on business demand but also with regard to the policy environment is slowing market evolution. So, while firm-level challenges are at play, uncertainties about how data-protection, credit-reporting, and open-banking rules (among others) will evolve in regard to sharing access to alternative data are to some extent discouraging new data providers and curtailing the pace of innovation.

At the firm level, data providers and issuers note a lack of expertise and a limited data scale as reasons for not pursuing or being more advanced in supporting data-driven finance. Some do not have the expertise or capacity to develop their own data-analytics capabilities. Hence, they look at partnering with external data-analytics providers. Others are trying to enhance the strength of the data provided by clients on their platforms or of clients in their portfolios by partnering, for instance, with ecosystem partners that provide small business services (such as cloud-based accounting, point of sale, and so on), or with data-analytics providers that partner with telco-data providers to develop lead-generation scores, behavioral scores, or other analytics.

The new data-analytics companies do not view themselves as "credit bureaus" or as competing with credit bureaus. Their products and services are complementary to those offered by credit bureaus in that they tap into the thin-file and no-file segments, or they provide lenders with greater insights into their own customers. Some of these companies are in talks with credit bureaus to supplement the services provided by credit bureaus, and some bureaus have indicated a reciprocal interest in exploring partnerships with the most promising and viable models.

Many of the innovative analytics products and services are still niche initiatives with small customer bases. Survey participants highlighted that client buy-in to their products and services relied largely on the regulatory compliance requirements that their clients faced. Since the alternative data market falls outside the purview of most regulators, hesitation to adopt new products and services safely, while ensuring compliance, is a limiting factor to uptake by regulated entities. Several analytics providers are still dependent on early-stage investors and have yet to prove the scalability and financial sustainability of their models.

5.10 Challenges to Developing Data-Analytics Markets

Some of the survey participants indicated that regulations get in the way of accessing certain registries or types of data. For instance, data from banks is generally not available to data-analytics providers, but it is available to credit bureaus. Regulations or internal governance rules may restrict third parties' access to data held by credit bureaus as well as a credit bureau's access to other data. For instance, in Singapore, the credit bureau does not have telco data, because, while the telcos would like to gain access to bank data in return for sharing their data, the regulator does not permit it. Telcos are disincentivized from sharing data with the credit bureaus. However, in the same market, any type of data can be accessed, processed, and shared if consumer consent exists. While open banking is not yet widely accepted in the markets surveyed, if and when it is adopted, these artificially created barriers to information may well become a concept of the past.

Lenders surveyed in each of these markets are cautious in considering new strategies and means of tapping into emerging data sources. For SMEs, in addition to payment performance data, lenders would like to get information on their suppliers, their buyers, their networks, and so forth. Questions remain, however, on the quality of alternative data or the ability to access data from suppliers or telcos (which is in part dependent on the size of lender). When it comes to certain types of alternative data, such as data from accounting platforms, point-of-sale systems, and so on, while in theory these sound great, the prevalence and usage of these platforms determine how extensive the data will be and whether it makes sense for a lender to invest in acquiring such data or analytics based on such data.

Some survey participants suggested that better industry coordination could help to formulate clearer policy positions and accelerate appropriate reforms. While some of the data-analytics providers are members of fintech or other relevant business associations, no specific data-analytics industry groupings were mentioned. In Indonesia, data-analytics companies have joined the Indonesian Fintech Association to enhance coordination and strengthen their voice in discussions with regulators.

Chapter 6

Survey Analysis

The survey has highlighted common themes, concerns, and issues. This section articulates preliminary conclusions about how the industry is evolving and summarizes the market concerns and challenges that have been raised by interviewees and that will probably need to be addressed by policy makers and private-sector participants in the near future.

6.1 Market Development

The roles of new and alternative data, data sources, and analytics will continue to expand, and their importance to increase. While there inevitably is some selection bias built into the range of companies (data and analytics providers) surveyed, it should be noted that incumbent banks and credit bureaus, as well as new data actors, expressed clear views (i) that new data sources were important, (ii) that the market for credit information would continue to diversify and evolve, and (iii) that the current policy and regulatory framework would need to adjust. So, although participants may not agree about what changes to market structure and policy should be made, consensus is growing that the status quo is not stable or efficient and that policy makers will need to orchestrate or support some kind of changes.

The key issues raised by new data, providers, and lenders are emerging. The most prominent issue raised by respondents concerned the legal and commercial terms under which new sources of data could be accessed, and by which market participants. Secondarily, some new lenders and financial intermediaries raised questions about whether in the future they may have (or be granted) direct access to established credit bureaus and other central registries (for example, for company records), to which access today is often restricted to members and/or to just domestic credit institutions. Credit-bureau operators and banks recognize that, while there are legitimate reasons for current access and membership restrictions, these will need to be reviewed. There is an implicit concern that, as the scope and scale of alternative data sources increase outside the reach of credit bureaus, the relative (but not absolute) value of credit-bureau data will diminish; some suggested that credit bureaus need to be free to expand and diversify their services to remain relevant.

Entity Type	Data Type	
	Established For example, bank lending/credit-bureau data	Emerging/alternative data For example, Telco records, firms' ERP, e-commerce, or sales records
Data providers/issuers • Financial institutions • Telecom and e-commerce • Enterprisetech • Other	Will banks have to provide access to data more widely—for example, via open-banking and finance regulation? Will telcos that operate mobile money also be treated like banks?	To what extent will non-banking data holders be obligated to provide fair access to legitimate users/ offer services to clients to share access?
Credit bureaus	Will open-banking requirements and the entry of new providers diminish the role of credit bureaus?	Will credit-reporting firms be free or required to cover more data and expand membership?
Data analytics and intermediaries	Will new data firms be able to access bank or credit-reporting data, or will access be limited to members?	Will regulation impose restrictions, standards, or obligations on new data intermediaries?
Lenders and financial institutions	How will the value of bank data change in relation to the predictive power of new and alternative data?	Will new sources of data and the role of new and different types of lenders erode the role of sharing records via credit-reporting systems?
	Will new lenders be required to report to credit bureaus more systematically?	

Figure 6: Emerging Issues Regarding Data Access by Type of Data and Entity

6.1.1 Integration Approaches

The survey has pointed toward the following five broad type of arrangements that will prevail or emerge for integrating new data providers and users into data ecosystems for financial services; these are not mutually exclusive.

1) **Bilateral agreements**
The simplest and most common approach to using new data that can be expected to continue is for financial service providers and new data providers (such as e-commerce platforms and accounting solutions providers) to work together directly and establish their own bespoke commercial agreements. This form of collaboration will continue to develop and be highly relevant, but smaller actors on both sides (for example, providers and users) find this approach to be difficult, mostly due to the costs of putting such arrangements in place and their relative bargaining or negotiating power. This can put smaller firms at a strategic disadvantage, often dissuading them from participating in the new data market altogether, favoring market concentration and depriving their users of opportunities to mobilize their data.

2) **Independent data intermediaries**
Incumbent and new as well as established data-analytics firms are already emerging as important facilitators of market evolution. They are able to contract with new data providers and sources, add analytical and security features to services, and combine new and existing services provided to banks and other financial institutions. New data providers, such as enterprise-tech firms, do express reticence about ceding too much control to these data intermediary firms, especially while they still have ambitions to grow and enhance their own data-analytics services, and questions remain about whether such data intermediaries need—or in the future may need—to be licensed or regulated. In this context, survey participants made positive references to the approach that consumer data-rights and open-banking policy frameworks are taking toward the licensing of third parties that wish to access consumer data.

3) **Expansion of scope of credit bureaus**
Credit bureaus are potentially well positioned to benefit from the alternative-data streams that are becoming available, by leveraging not only their deep understanding of the common principles of data sharing and their existing sophisticated IT systems, infrastructure, expertise, and deployment capabilities but also their understanding of data-privacy and consumer-protection obligations. Hence, they may expand the scope of the services that they provide to the market. Many surveyed companies noted that this option has strong economic logic, but issues regarding their mandates, ownership and control, and incentives were raised as potential impediments to credit bureaus being able to fulfill a more inclusive role in the new and emerging data economy. An expansion of their role could be a complement to competition from new service providers.

4) **New centralized platforms**
In some jurisdictions, there are discussions about creating new networks or centralized data exchange hubs, especially for SME business data, to ensure a more open data market. Plans for such new institutions are still in very early stages of discussion. They would probably be based on opt-ins by firms to share data and would not supplant the obligatory reporting of exposure by banks. Most private market survey participants indicated sympathy with the intent of such plans but expressed skepticism about the practicalities of creating new structures, especially if they require data sharing with a centralized entity that would also have a mandate to cover the whole market, thereby potentially squeezing out private-sector third parties.

5) **Decentralized financial and data networks**
Another emerging approach is to support decentralized finance structures through which access to data or credentials is controlled by the data subjects themselves but is verified by its issuers. This kind of data portability may be supported by the use of verifiable credentials. [25] This approach was being developed by one surveyed company as a means to enable data "issuers" and "users" to exchange information—as opposed to raw data—without necessarily sharing data with a third-party analytics firm. Verifiable credentials can enable bespoke enquiries to be made about a client without the actual underlying data being shared. This is similar to the practices employed by credit bureaus—for example, in providing scores, but verifiable credentials provide a decentralized mechanism for verifying the authenticity and legitimacy of both the data issuers and the requesters.

These scenarios may be useful for structuring further research, assessment, and debate while developing recommendations for policy makers and market participants.

6.2 Data Access and Fragmentation

One set of issues voiced by survey participants, especially lenders, concerns data fragmentation. A key objective of credit information-sharing systems is to reduce asymmetries and provide lenders with information about the creditworthiness of borrowers. Such systems can enable lenders to have a more complete picture of the overall exposure of borrowers, from reliable sources, since the major lenders in most markets report into these credit bureaus. However, as the array of new lenders and types of lenders increases, it may be necessary to extend reporting obligations to them alongside traditional lenders. This may also imply capturing data from foreign as well as domestic lenders about their exposures, and from non-bank creditors such as suppliers or their trade finance partners. If new data from new sources of lending are not covered, these structures are weakened. Lenders may instead need to connect to a multitude of data providers and rely more on alternative data types to assess risk. The market may become more complex, and the costs of operations can increase. It may take time for new consolidated providers to emerge and reestablish more efficient arrangements, especially if regulation hinders their emergence.

New types of lenders are not always required to share information about their portfolios with credit bureaus. Whether person-to-person lenders, fintechs, or others, institutions that lend on the basis of information sourced from their proprietary platforms may not be sharing data on their exposure. As a result, other lenders may have a less complete picture of their borrowers' profiles than they did before. For instance, if a merchant on an e-commerce platform is receiving financing from that e-commerce platform provider (based on the merchant's track record on the platform), this financing arrangement may not be available to other lenders. These other creditors will still rely on information disclosed by the merchant and/or the credit bureau(s), where they exist, for an accurate understanding of the merchant's ability to meet any other credit obligations. The issue of information fragmentation is therefore exacerbated by the lack of any common standards or reporting requirements across all types of lenders, which would create a more complete picture of the borrower.

New data providers or issuers lack strategically neutral and competent third-party channels through which to provide access to their clients' business data. This is especially true for smaller firms that may have fewer resources to invest in managing their data or have less market power to negotiate favorable terms with lenders. In the absence of regulation that provides end users with more control over their data—for example, through access or data-portability regimes—demand for appropriate third-party intermediary structures may be weak. Larger financial institutions and e-commerce platforms, for instance, may reap the biggest gains from new data ecosystems, because they can afford to invest in the means to police access and usage and build trust and use their scale to integrate data across different functional domains. Small firms may not be able to earn enough revenue purely from value-added data services to justify these overheads.

6.3 Security, Integrity, and Legitimacy

6.3.1 Data Quality

Market participants—providers, intermediaries, and users—consistently raised questions about how to ensure the quality, reliability, and authenticity of new data. New data providers may have less experience or skills to ensure data accuracy, and until they see its revenue-enhancing potential, they may underinvest in developing its potential. New intermediaries often face long phases of development in which banks test the usefulness of new scoring and data, and early on, it is difficult to assess the quality of new providers and their models. Many of the new data issuers or providers admitted that they were only beginning to understand how to mobilize data and, hence, that they lacked clarity on what aspects of quality, accuracy, or completeness were important and what gaps they might have to fill to satisfy financial-sector users. The survey also suggests that there is limited awareness of the requirements in the financial sector with regard to the duration and robustness of record keeping, the need to support audit trails, and financial service providers requirements to verify or rely on a third party's check of the authenticity of data (for example, for KYC). In some market segments—for instance, with regard to account aggregators in India or in the fintech domain in Indonesia—industry associations are playing a role in developing guidelines or standards for data management and access, but most new data issuers are not covered by relevant industry associations and/or they do not have an active effort to develop such standards.

6.3.2 Legitimacy

Market participants generally believe that not all data should be freely accessible, even if access to it has been provided with the consent of the original owner of the data. Some eligibility criteria and vetting are widely seen as necessary to ensure that only bona fide firms with legitimate functions and needs are allowed to access data, but there are no clear and dominant views on what such criteria would look like or who would govern, operate, or enforce any rules. However, there is broad recognition, even among the financial services actors, that the scope of such rules will at least need to align with or stretch beyond the information-sharing rules applicable to financial services authorities.

6.3.3 Liability and Accountability

A key aspect of legal and regulatory frameworks governing the sharing of credit information is that accountability is assigned to the relevant stakeholder in the system. For instance, if a data provider were to submit incorrect data to the credit bureau and either the bureau detected it or a consumer disputed it through available dispute mechanisms, the onus of checking the error and rectifying the data in case of a real error would fall upon the data provider. Similarly, these frameworks assign responsibilities to the credit-reporting service providers (credit bureaus) and users of the system, and the frameworks hold them accountable for failing to meet these responsibilities.

With regard to new data and models, lenders take almost full responsibility for their use. New data providers and analytics firms in the survey acknowledge their responsibility for respecting data privacy and protection rules, but it is financial institutions that bear the credit risk and other consequences, for instance, of inaccurate or low-quality data or data models. While this may be appropriate, many survey participants noted that this situation creates understandable reluctance to test new models and providers. Since new models can demonstrate their value only by being tested, new firms and data often struggle to get on the first rung of this ladder. Hence, some new data-analytics providers have either turned to new less risk-averse lenders or participated in risk-sharing arrangements during the early stages of deploying their models.

In a more democratized world of credit-scoring models, it may be harder to identify the source of problems and assign accountability. If each and every entity is an independent agent, either sourcing data, providing data to third parties, or building models based on alternative data points, this issue of accountability will be accentuated. A lack of definite categories of data providers—such as banks, microfinance institutions, and utility providers—will make it more difficult to apply a coherent legal framework. Every entity that either provides a product or a service—be it an e-commerce platform, a lending platform, or a payments solution provider—is now a potential data provider, data user, or provider of scoring solutions. In most markets, these different entities fall under the ambit of different supervisory agencies or, in some cases, none at all. The identification of responsibilities and assignment of accountabilities is therefore very complicated. From the survey, it appears that all players but the traditionally regulated entities, such as credit bureaus and the financial institutions, are responsible for adhering to a patchwork of laws, interpreting them as best as possible and implementing policies and procedures to comply with the same. As new players emerge, therefore, the risks of incorrect data, inaccurate models, and decisions are accentuated, thus posing greater risks for consumers.

Questions were also raised about the accountability for model oversight. Based on the survey results, the companies that develop scoring models rely largely on their in-house expertise to test and validate their models. There is no external oversight on these models. And even if there were external oversight, given the complexity of the models and the degree of automation (where artificial intelligence and machine learning are used), the market perception is that regulators and supervisors are not necessarily equipped to supervise or test these different models. To paraphrase one survey participant, "[the regulator] leaves it to these companies to do whatever they want and run it as a business. It's up to these companies to develop the rules and the financial institutions to use it as they see fit. Unless something happens—like credit scores that result in fraud or excessive credit losses, the regulator does not get involved."

6.4 Data Privacy and Protection

Most firms anticipate changes to the scope and structure of data-protection laws and regulations. Of the companies surveyed, the traditional credit bureaus and regulated lenders follow the most stringent measures in upholding data privacy and consumer protection. For the most part, they are required to do so under the relevant legal framework. These entities also have dedicated customer-service desks to handle customer queries, concerns, and complaints. Of the companies that provide third-party data-analytics solutions, a large percentage relies on the client's privacy policies and consumer-protection measures. For instance, they rely wholly on their clients to obtain consent prior to sharing the data with them. Most of the entities that rely on third-party analytics providers for scoring models anonymize the data prior to sharing it, with the objective of masking the identity of the underlying borrower. However, anonymization of data has been known to be not completely foolproof. The data-analytics providers themselves are responsible for the security and integrity of their own systems, internal governance controls, and other compliance requirements, where relevant regulation exists. In the absence of coordinated policy or regulation, however, this results in varied approaches to privacy and consumer protection with little oversight.

6.5 The Level Playing Field

A final issue raised is that different rules and access conditions may apply to different kinds of actors. In this evolving data space, financial service providers may be subject to stricter regulations, including obligations to share data with regard to conduct of business and legal requirements; bigtech firms, on the other hand, are (for now) generally not obliged to share data with third parties. When they do share data, the terms on which such access is provided may be considered unfair. Established data-analytics firms, intermediaries, or credit bureaus may also be subject to different rules and regulations depending on the scope of information they deal in and the jurisdiction in which they operate. Overall, there is a sense that the playing field is shifting and that it is certainly not level. While there is recognition that financial data may need to be treated differently from nonfinancial data, the survey underlined the expectation in the market that policy will inevitably need to catch up and take steps to realign and level up the market. [26]

Chapter 7

Policy and Market Development Considerations

This section provides a preliminary discussion of aims and issues that policy makers and industry players should consider as they think about how, together, to further develop the market. While this section does not propose specific policy actions, it does make recommendations about emerging problems that policy makers should be attempting to address, notes some of the options and trade-offs under consideration, and identifies potential approaches that warrant further discussion and research. Overall, these considerations focus on market structure and regulatory issues that will be of importance in managing the transition from existing credit-information frameworks toward the more open and diversified data ecosystems in which financial services are increasingly operating.

Most of these aims and issues constitute a subset, or articulate a specific application, of policy issues that are being considered more generally within the context of the data economy, such as data-protection and trade regimes. As many jurisdictions are working in parallel on these policy issues, it is important to understand the role of new data, processors, and users in value creation and competitive advantage. [27]

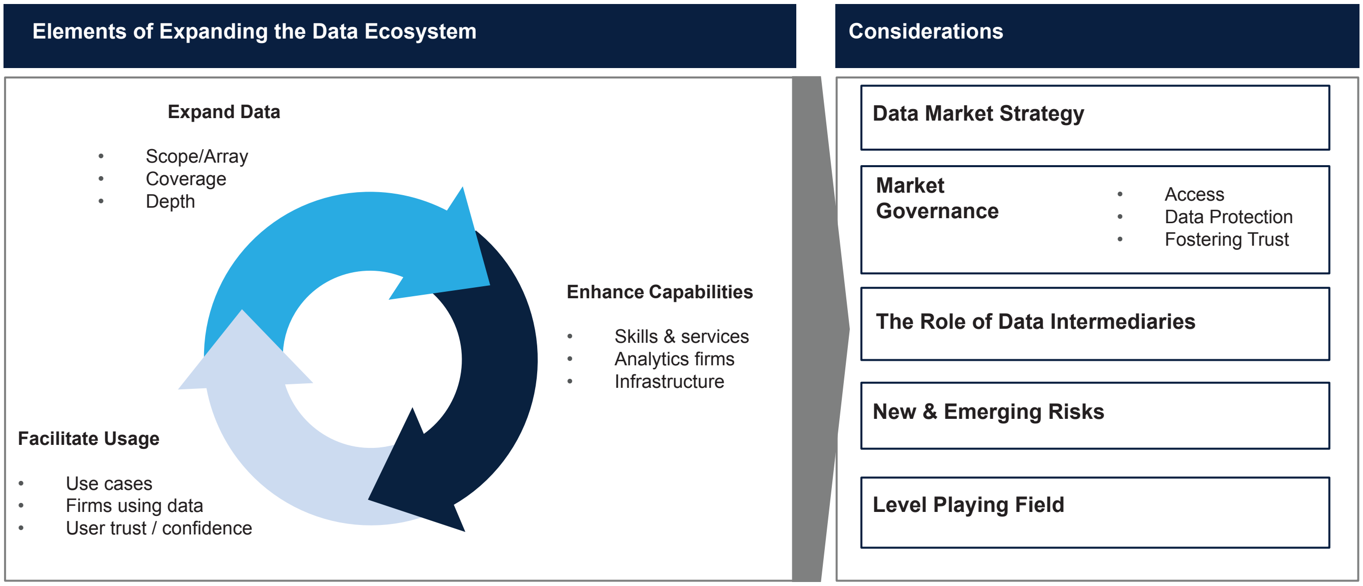


Figure 7: Overview of Considerations

7.1 Expanding the Data Ecosystem for Financial Services

The question is not if but how. Many countries are now articulating broader “data market strategies” that encompass several dimensions. Policy makers and private-sector actors are concerned primarily with three supply-side elements of the market. First, there is an interest in expanding the array and depth and coverage of data that can be securely and efficiently mobilized in the economy. This includes, for instance, moving beyond basic and relatively standardized transaction and account balance data to enabling at the very least use of data on sales, procurement, logistics, and customs declarations. In more specific industries, such as health care or agriculture, other data sets can be useful for assessing and monitoring financial risk. Second, it is necessary to foster the development of the intermediaries and their capabilities and skills needed to provide value-creating analysis of data. In the new business models of the data economy, these are important activities that create competitive advantage and local high-value jobs and revenues. Supporting a dynamic and contestable market for intermediaries may also require putting in place some forms of legal and institutional infrastructure that would be inefficient for each firm to create by itself. Third, expanding the data market implies also fostering use cases and the role and variety of firms that use data and analytics as key assets in their production model. This includes not just financial service providers but many of the real-sector firms that are both at the source of and users of data needed for financial services algorithms. Fostering usage also requires the confidence of end users (customers), which can in turn can help to expand data availability in a virtuous cycle.

Both incumbents and newcomers can benefit if they are able to apply new data types to the provision of financial services, but market structures influence the relative distribution of those gains; the results can be asymmetric. In developed economies, a key issue has been about a lack of competition in the banking sector and getting more structured and robust third-party access to bank data. This is also a concern in the markets covered in this survey, but the relative market power of newcomers—for example, digital platforms such as Grab and Gojek—is greater than it is in, for instance, Europe. Banks, on the other hand, are concerned about their ability to compete with bigtech platforms that increasingly have more power over data but are not subject to the same constraints and obligations as banks. In many markets, plans are already emerging for the expansion of data portability and access right to domains outside finance but still of relevance to financial decision-making. As an example, the Korean payment systems operator KFTC has indicated that it intends to help intermediate nonfinancial industry data of relevance to the development of the internet of things; the Australian Consumer Data Right Act is designed to apply to data held by electricity companies and other utilities; and in the European Union, the emerging data strategy speaks of enabling data portability and utilization in other areas of the economy, including health care and industry applications such as the internet of things.

The rules and regulations surrounding new financial data-analytics providers and their operations continue to evolve. There does not appear to be any single approach to dealing with these new players, except through the broad principles of data privacy and protection. On the whole, policy makers and regulators have sought to support greater innovation and refrained from introducing new regulations preemptively. However, regulatory uncertainty is also creating an issue with uptake of the solutions provided by these new fintechs and data-analytics companies. Surveyed lenders indicated that uncertainty in the regulatory environment was a key factor in determining whether to rely on third-party analytics companies. Since regulated lenders are ultimately responsible for their decisions and accountable to their regulatory authorities, they tend to adopt a more risk-averse approach to incorporating information from alternative sources or credit-scoring models. Consideration should therefore be given to providing more clarity on the governing legal and regulatory frameworks for credit information sharing. This may focus on defining which data types and services warrant access controls and standards of behavior and then providing some register of data-analytics companies that meet or comply with such rules or guidance. It may also be necessary to provide greater clarity on the data rights, legally binding forms of consent, obligations, and enforcement mechanisms or penalties that apply to the firms providing, accessing, or using new data. These should be proportionate and aligned with equivalent rules already applicable to credit-reporting data; potentially both will need amendmentsamended).

7.2 Data Market Strategy

Many governments are articulating broader policy approaches toward data and the digital economy. Data that is relevant to financial services, such as for risk scoring, is only one small subset of this broader policy debate. Access and usage of data for financial services should be considered within this broader context. Even in markets that have already reformed some aspects of financial services regulation to address the new data economy (for example, such as under the EU PSD2), there is recognition that reforms need to be broadened to address similar data access, usage, and protection issues in other parts of the economy.

Within the context of this survey, participants noted that the following two aspects of such data strategies should be brought to the attention of policy makers:

- **Data is a productive and strategic asset.**

Well beyond its application to financial services, data is being recognized as a valuable input to, and often a prerequisite for, innovation. Data is needed for advances in artificial intelligence that can drive new industries and technologies. Developments in areas such as driverless vehicles, energy efficiency, and medical research, as well as in finance highlight the importance of having rich interoperable data sets that can be used to refine new technologies. While governments should not try to prescribe how data can create value, they should heed calls by industry and researchers to enable the broader usage of data in a secure and efficient manner. Hence, many governments are trying to address overarching and sector-specific opportunities to unlock the value of data for innovation. The approach to data-access rights in Australia highlights this view that data needs to be seen as an asset that belongs to the data subject, who may wish to use it across multiple domains of the economy.

- **The public sector can play role in enabling the market for data.**

While it should be acknowledged that the market is still evolving, market innovators lament the lack of access to data, low levels of digitization, and incompatible standards. Data is often still trapped technically, commercially, and legally in disparate silos. And the legal scope to access and use data is often unclear for many firms. Governments may be able to play a role in addressing some of these market failures.

Government itself is an important and, sometimes, the sole source of data that can be instrumental in enabling new business services. It can potentially lead the way in stimulating the market through better access to national ID, payment, and other systems under public control. Access to certain types of data on commercially fair and secure terms might need to be mandated (as has been the case in open banking) to provide greater operational control to end users and allow for more competition in concentrated sectors. To support the provision of scalable and efficient service, there may be a role, as in many other areas of the economy, for standards—in this case, for functional and technical data standards that support interoperability. Moreover, the legal rights and obligations associated with data access and usage, as well as their enforceability, require clarity that only legal systems can provide. Lastly, government may need to play a role in recognizing the digital standards for contracting and identification that will stand up in a court of law. Large-scale digital enterprises have in effect provided private-sector solutions to many of these challenges, within their own closed networks, and as the industry matures and diversifies, some of these issues may be addressed through private-sector coordination, but in many instances, private-sector players are also looking to government to play a role, at the very least as a catalyst and advocate for broader market development.

7.3 Governance

The data market may require economic or institutional governance arrangements to operate effectively. While private markets may emerge, some schools of thought accord an important role to the institutional governance arrangements that frame a market and help it to operate safely and efficiently. Various dimensions and forms of governance are still being discussed and tested in this new area. A few key issues and approaches for consideration include (i) rules governing access to data—by whom, under what conditions, and to what data; (ii) data-protections and privacy rules that individuals on their own cannot police or impose; and (iii) other elements of market arrangements that can help to build trust in data and counterparts operating in the market.

7.3.1 Data Access

While the importance placed on data rights varies by country, greater clarity on the position of regulators in a given market would help. Some markets have developed very strong mandates that explicitly accord greater rights to end users to access, use, and share their data; other governments have chosen a much more hands-off approach and left it to market forces. Much of this has been enacted through open-banking-type regulation initially applicable to the banking sector but gradually being further applied to other parties. It is still too early, on the basis of empirical evidence, to advocate strongly for a particular position, but either way, clarity of the position taken in a given jurisdiction can only be helpful, even if policy makers retain the right to revise their approach as new evidence and market developments emerge. This is a view supported by the respondents to the survey.

7.3.2 Data Protection

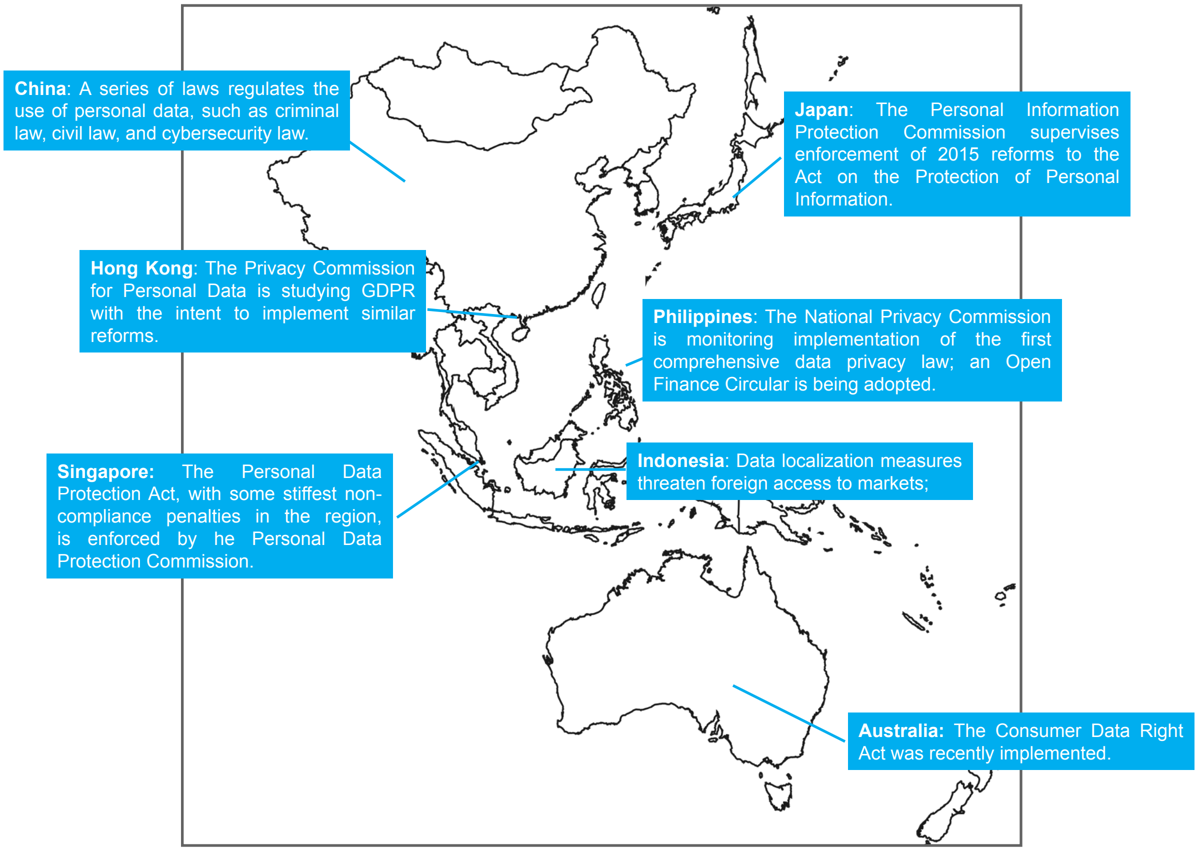
Consumer data-protection legislation and education measures will need to evolve in tandem with specific data market issues related to credit information and financial services. Based on the survey, it appears that basic principles around consumer data protection and those covering privacy and bank secrecy are being applied through broad legislation (see figure 8 for examples of different legal and regulatory frameworks) or bank-specific rules, but that, so far, there is a little guidance in terms of implementation or checks to evaluate the effectiveness of existing measures implemented by the different participants. Some considerations for policy makers include the following:

(i) Proposing measures to strengthen the oversight of nonfinancial data providers in terms of how they collect consent, inform customers, and how they store such consent.

(ii) Setting up frameworks to guide the use of alternative data—including defining its scope, purpose specification, and limited-use principles, in addition to the requirements for ensuring the security of such data. Such frameworks may set penalties for the misuse of such data.

(iii) Strengthening the existing regime of data protection and ensuring that consumers are truly aware of how their data is accessed, used, for how long it is retained and for what purposes it can be used. Many participants expressed the view that consumers should be informed of their rights to their data, including the ability to check and challenge such data where the data is believed to be incorrect. Efforts may be needed to educate consumers about their scores and how these are derived. Also, consumers' control over the data may become a new norm. Hence, appropriate policies, regulations, and system capabilities to ensure data portability from one processing system to another needs to be contemplated by the industry stakeholders.

Coordination may need to be enhanced between supervisors of credit-reporting systems and, where they are regulated, data-analytics companies supporting credit underwriting. In some markets, the relevant data-protection authority is tasked with overseeing the activities of all data market participants. (See box 1 for an example.) Given that data-analytics capabilities are emerging across different industry verticals, it may not be practical or feasible for a single data-protection commissioner to oversee and effectively enforce laws or regulations. Enforcement capabilities may need to be developed within different industry regulators, and the main data-protection commissioner could play a role in coordinating the overall enforcement function.



China: A series of laws regulates the use of personal data, such as criminal law, civil law, and cybersecurity law.

Japan: The Personal Information Protection Commission supervises enforcement of 2015 reforms to the Act on the Protection of Personal Information.

Hong Kong: The Privacy Commission for Personal Data is studying GDPR with the intent to implement similar reforms.

Philippines: The National Privacy Commission is monitoring implementation of the first comprehensive data privacy law; an Open Finance Circular is being adopted.

Singapore: The Personal Data Protection Act, with some stiffest non-compliance penalties in the region, is enforced by he Personal Data Protection Commission.

Indonesia: Data localization measures threaten foreign access to markets;

Australia: The Consumer Data Right Act was recently implemented.

Reproduced from Hogan Lovells (2017); DLA Piper (2017) ADMA (2017), with selected updates

Figure 8: Overview of Data-Protection Laws

Malaysia passed the Personal Data Protection Act in 2013 and has a data-protection commissioner who is empowered to implement and enforce compliance with the personal data-protection laws. The act gives the commissioner powers to inspect the systems used when processing personal data. The commissioner may require a record of consent from the data subject, policies on data retention, data integrity, security policies, and so on. Violations of the act can result in administrative and monetary penalties. This is not unlike the list of requirements that traditional credit-reporting service providers or credit bureaus are required to meet for the handling and treatment of personal data.

7.3.3 Fostering Trust in the Market

The survey highlighted some of the areas in which market participants suggested a lack of trust creates inefficiencies. In particular, survey participants raised questions about (i) how to enhance trust in new data, (ii) the credentials of data intermediaries and providers, and (iii) how industry self-regulation could or should play a role in fostering market development. They provided examples of mechanisms they thought may play a role in addressing these challenges.

- **Trusting new data**

There was a sense that by licensing intermediaries, establishing best practices for them to follow, and having market structures that set the right incentives for intermediaries to provide reliable data and analytics, third-party intermediaries could play an important role in providing trusted data, helping to vet providers and staking their reputation on providing reliable analysis and outputs.

- **Trusting intermediaries**

While in principle market participants may be open to use and share new data, they may lack the means, especially with remote and automated processes, to verify the identity and check the credentials of third parties from or to which they provide/receive data. Survey respondents raised questions about how you do this in an efficient manner, especially if such entities and their activities in the data market are not regulated. How do you reduce the uncertainties and costs of banks' lengthy and repetitive due-diligence processes, and what criteria are important?

In the absence of a comprehensive licensing regime, participants, especially banks, need other ways to assess the legitimacy of data sources, issuers, and analytics service providers. These checks often represent sunk costs that each market participant has to incur, and they are "non-rival" goods that could be better mutualized. It may be inefficient and impractical to set criteria for and to license all of the new actors in these emerging data ecosystems. It may not be clear which activities should be covered, or under the mandate of which authority this would be achieved, so some survey participants are already investing in private, alternative, decentralized solutions that enable banks to field enquiries from other participants and benefit from the checks that other market participants have already performed.

One surveyed firm provides services for issuing and checking digital "verifiable credentials." The technology and scheme operators supporting verifiable credentials enable "issuers" of data to tokenize or "credentialize" answers to specific data queries and provide "users" with the means to request data and via a third party verify that the information has not been tampered with. These solutions can provide for further updates and track inaccuracies or cases of fraud over time. The approach is gaining ground and has already been applied to the digital issuance and verification COVID-19 checks and as a means to enable casual workers to collect records from former employers that new employers can verify.

- **Industry self-regulation**

One of the key themes emerging from the survey was the lack of regulatory clarity or certainty. Many survey participants indicated that self-organizing at the industry level would allow them the opportunity to exchange experiences and concerns among themselves. All the players interviewed showed a commitment to adhering to basic rules around security, data protection, and consumer privacy. However, since these new models involve new types of data and assumptions that go into the use of them, an industry association would also provide the players with a platform to agree on ethical or responsible guidelines for the access, use, and distribution of data. Many countries now have new industry associations in such areas as blockchain or fintech, but fewer cross-cutting coalitions at this stage are regrouping the broader stakeholders in open data. [29]

In the absence of clear legal and regulatory frameworks or industry standards, industry participants could develop their own self-regulatory approaches or standards. While different markets are still evolving in terms of regulations, data-analytics companies should develop reasonable internal and external compliance policies and procedures, with an expectation that this space is going to become increasingly regulated. Such self-regulation and standards may also help inform and direct policy determination and subsequent regulation. This may entail more cooperation between regulators across different sectors (financial and telecom, for instance) or the adoption of open-data standards to provide more control to the consumers at the origin of the data or to whom it pertains, to decide what information can be shared and with whom. This may also include aligning incentives of different types of data providers through greater outreach and awareness raising, in which associations may also have a key role to play.

Individual companies may also need to develop their own data governance frameworks using available local and global benchmarks. This should be in addition to and complementing government-led strategies. Frameworks should classify the different types of data in question, prescribe limitations on how such data may be used, what data will be shared, and the necessary controls for ensuring quality, accuracy, and consistency, as well as the privacy and security of underlying data subjects. It could be helpful to indicate technology tools as well as propose a line of accountability and assign key roles for different individuals tasked with handling data and related processes.

7.4 The Role of Data Intermediaries

From the research, consensus appears to be growing that new and existing data intermediaries need to play a role in expanding the market. As Coyle and Li also note in their recent paper on the data economy, "an appropriate framework for access to data could motivate gatekeepers to invest in market mechanisms that increase the utilization of data."[30] Bilateral arrangements between individual data sources and a financial service provider that uses that data are not scalable or efficient. They can not only have operational drawbacks but also dissuade smaller data providers, out of strategic concerns, from taking part in the market. The relative size of platforms versus niche data providers can result in a winner-takes-all outcome that smaller firms will be reluctant to support. So questions arise about how the role of data intermediaries (or "gatekeepers") can be facilitated and what if any regulation or legal frameworks should apply to them to incentivize investment and broader usage of data. Some markets outside the survey region are adopting open-data approaches that involve defining and licensing certain types of data intermediaries (for example, account information service providers) that have motivation to make better use of data while at the same time providing greater power to consumers.

A sophisticated web of different types of intermediaries already exists, providing overlapping roles in the evolving data ecosystems. Some firms support data providers and their clients by cleaning and structuring their data in a way that it can be used. Others may help to verify identity, control, and secure access to data requests by third parties; some such firms are licensed in the European Union as account information service providers. Then there are data-analytics specialists that have the domain expertise necessary to interpret raw data and draw meaningful insights or scores from it. The end users or consumers of the data—for example, lenders—may never actually need to see the data itself. The emerging practices in the market do not require centralized data hubs or repositories but rely more on an ecosystem of independent intermediaries. It is important that policy works with these evolving structures and provides the right incentives for their development while also affording meaningful protection to consumers.

Some jurisdictions—such as the United Kingdom and India[31]—are contemplating the creation of new data networks for information sharing. Based on this model, borrowers would be able to connect to diverse data sources with whom they hold relationships (banks, utilities, insurance, and public data sources, including identification authorities, social media, online reviews, and so on) and provide permissioned third-party access to entities with whom they are entering into contracts or engaging for access to services. Such access would be encrypted, and specific data fields would be available for a defined period. The United States' Small Business Association, as a part of its digital strategy, has been supporting the Open Data initiative, with an aim to make data resources available for public use. Some examples of data sets available for use are Dynamic Small Business Search, SBA Disaster Loan Data - Superstorm Sandy, SBA Enterprise Datasets, Small Business Size Standards - NAICS Data, and Small Business Administration (SBA) Loan Program Performance, among others.

7.5 New and Emerging Risks

Data users are concerned about the opacity of new models and their automated nature. Models that are driven by machine learning may produce results that are not fully transparent or anticipated by their managers and could lead to unintended discrimination. Regulators are challenged in assessing or overseeing these models and testing them for effectiveness. While models used for lending can and will be regularly tested in terms of predicted versus actual default rates, there may be model selections, such as rejections, that may be more difficult for applicants to foresee and for which it may be difficult to address customer complaints. On the other hand, with a dynamic and open market in both data and data-analytics providers, it may be easier and less costly for lenders to run several models in parallel and therefore contribute to better modeling overall. Also, it should be noted that specialist file-enhancement providers are helping more excluded borrowers to manage their own data profiles better.

A few considerations for policy makers in this regard are as follows:

(i) Support the development of a clear framework for the use of new technologies (such as artificial intelligence and machine learning) in building alternative credit-scoring models in terms of the responsibility for their outputs and obligations of transparency and consumer protection. The Financial Stability Board also highlights the need for enhanced efforts to improve the interpretability of artificial intelligence and machine learning not only for risk management but also for greater trust from the general public as well as regulators and supervisors in critical financial services.

(ii) Require analytics companies to provide equivalently adequate disclosures (perhaps on a tiered basis) to different stakeholders in the system. This should not be technology specific and should apply to other models that do not use new techniques, but new methods may require further clarity. For instance, regulators may require more disclosure to be able to assess and test underlying models effectively. Lenders using these models may require a different level of disclosure to gain sufficient comfort in adopting these models. Borrowers must have sufficient information to be able to challenge the results of a model as it relates to them.

(iii) Provide more guidance on the responsibilities of data-analytics providers in terms of governance and security as a means of providing more comfort to the users of these analytics services and distributing the risk more appropriately. External oversight or outsourced checks can also support the industry in following minimum rules of conduct.

One approach that authorities may consider is employing industry testing environments. Many jurisdictions are using technical and collaborative frameworks and systems to inform market and regulatory design reforms. Some markets have put in place sandboxes where data providers and analytics companies can test their new data sources, technologies, and methodologies. (See box 2 for an example.) Companies that successfully meet the sandbox criteria can demonstrate to potential users greater confidence in the reliability and efficacy of their models.

The Infocomm Media Development Authority of Singapore provides a data regulatory sandbox through its Data Collaboratives Program to support businesses in establishing trusted data-sharing partnerships and to explore and pilot innovative uses of data in consultation with the authority and the personal data protection commissioner. The sandbox is a safe environment for different data custodians and processors to pilot new data sources and test new technologies on their data sets, and it provides the governance frameworks needed to ensure that the data sets neither are in noncompliance nor risk the safety and security of the underlying customer data.

7.6 Level Playing Field

Policy makers should consider how reforms interact with market structures and to what extent they need to rebalance rules to maintain or create some form of a level playing field. Generally, the market expects the same rules to apply to different companies conducting the same activities, and there is common support for the principle that rules should be risk adjusted—that is, proportionate to the risks that a given activity generates. However, views often diverge on what risks or other externalities (positive or negative) firms create or how significant they are. Are new entrants free-riding on the risk management of regulated banks? Are banks unduly sheltered from competition because of regulation? Are bigtech firms misusing their market power to block competition? These are the kinds of questions often raised. In the changing environment of credit and financial data and analytics, participants recognize that legacy regulatory classifications of their services and activities may no longer align tightly with the existing practices.

One instrument of leveling the playing field in data is to apply the reciprocity principle. Policy makers in Australia, [32] for instance, have designed a regulatory framework for consumer data rights that applies the principle that "those (institutions) who wish to become accredited and receive designated data at a consumer's request must be willing to share equivalent data, in response to a consumer's request." This is designed to grow the scope of data available for consumers "and to ensure that those that join the system also contribute to the system." Applying this principle hinges on a sectoral-level interpretation of "equivalence" so that kinds of data that are distinctly different from those already covered by the legislation cannot be required to be shared until a formal sectoral assessment process has been completed.

Greater clarity and consistency may be needed in the way that regulators apply the principle of same activity-same rules. Many fintechs and data-analytics providers provide data that is used in lending models of regulated or unregulated lenders. In that context, they may be assigned responsibilities not unlike those that are accorded to credit bureaus. The current distinction between traditional credit bureaus and these companies appears to lie in the types of information that they handle and treat. In reviewing the regulation of fintechs and data-analytics providers, some of the responsibilities that governments may want to consider include the following:

(i) Adhering to minimum guidelines for ensuring security of systems, databases, and infrastructure

(ii) Having minimum requirements for consumer privacy and data protection, including obsolescence of data, retention periods, consumer-support functions as appropriate, and consent requirements

(iii) Having explainable[33] models, including rationale for input variables

(iv) Creating governance structures for the collection, storage, transformation, and usage of data

Relevant authorities may consider expanding access to central registries and systems to fintechs and third-party data-analytics providers. This could be a means to level the playing field. Banks generally have access to infrastructure to fulfill their obligations to confirm identities as well as to enhance or cross-check risk models with other systems, such as for tax or social security. Jurisdictions may want to consider whether third parties should be accorded more general access to such sources and, if so, based on what criteria. Policy makers may therefore want to develop (i) guidelines for access, including minimum requirements that data users (scoring companies, credit bureaus, and analytics companies) should satisfy to access such information, and (ii) data standards, for instance, in regard to coverage, disclosure to and rights for consultation by individuals, accuracy, frequency of updates, demonstration of relevance for an enquiry, and clarity on the application and in existing financial regulations.[34]

Security

Chapter 8

Conclusion

As data may be the "new oil," [35] it continues to spawn development and investment in related businesses for its extraction, refinement, and distribution, as well as derivative products. More recently, The Economist noted that data has been compared perhaps more aptly with "sunlight because soon, like solar rays, they will be everywhere and underlie everything."[36] Either way, while its power can be harnessed for good, each source of energy comes with its own dangers and requirements to retool our market structures and adjust our behaviors. As such, it is important to take stock of the ways in which actors in the economy are using data or perhaps struggling to make better use of it in ways that can further aims, such as financial-sector development, that policy makers generally strive to support.

This paper has summarized insights from interviews conducted as part of an interim stocktaking. It has focused in particular on actors extracting new data and putting it to use in SME finance in Southeast Asia. The survey shows clear and rising demand for using new data. The aim was to provide empirical insights into what is happening in the markets that may help to inform ongoing policy debate about how to improve market outcomes in markets where data sources and business models continue to evolve.

The exercise has revealed some of the challenges of data extraction, refinement, and distribution. Some firms have data that they would like to share—or make accessible—in ways that serve them and the interests of their customers, but they may not want or be able to find cost-effective ways to provide access to it to multiple institutions that can use it. Users of such data can often put it to good use only if it is merged with other sources in scalable ways and using expertise they may not hold. Bigger firms with market power and sufficient skills and capacity are overcoming these hurdles. Smaller, more agile firms are often the most effective developers of new business opportunities, but they often face challenges to scalability. Trusted and specialized intermediaries can play an important role between data issuers and users.

Demand for and usage of new data is in part tempered by lack of clear regulatory guidance or at least a road map that can inform investors' strategies. While larger firms have had the economic incentives and resources needed to create private network solutions to mobilize new data, this trust may be waning. Meanwhile, smaller firms are in a weak position vis-à-vis these firms and at a disadvantage when it comes to using or providing access to new data sources securely. Data issuers and analytics companies are often unsure how regulations will apply to their activities in the near future, what they will be held responsible for, and how they will be treated vis-à-vis other regulated players (such as credit bureaus) in the market. A lack of regulatory clarity impedes uptake of their services by financial service providers. Further, financial service providers would benefit from greater distribution of risk and responsibilities while adopting data-analytics services.

While waiting for legal and regulatory frameworks to evolve, data and analytics providers may benefit from developing industry-led guidelines themselves. Self-associating and developing rules or guidelines for their own industry could align participants with local and/or international frameworks for consumer protection and privacy, and standards for data quality, management, and governance. The general principles for credit reporting can continue to serve as fundamental principles for all flows of information related to credit-underwriting processes.

Policy makers and regulators will need to play a more proactive role in articulating and shaping data ecosystems in financial services. They will need to balance objectives of safety, security, and integrity with the opportunities presented by innovation. As consumer mobility and ownership of data gain greater significance, consumer data protection will most likely continue to be strengthened. Industry players—data providers, users, and intermediaries—should play a more active role in shaping the market, potentially through stronger industry policies, procedures, and functions to address consumer queries and grievances.

Appendices

A. Survey Firms and Business Activities

This table provides an overview of some of the firms that responded to the survey questionnaire, indicating their main area of activity and the market(s) in which they are based or operate and that were considered in the context of this paper. Note that some firms chose to withhold their names from disclosure.

Name	Business Activity	Home or Main Markets
Alliance Bank	Local retail bank	Malaysia
AMRET	Local microfinance bank	Cambodia
Aspire	Trade and SME finance platform	Indonesia, Singapore, Vietnam
Axiata	Telecoms and media services	Several markets in Southeast and South Asia
CP Bank	Local retail bank	Cambodia
Credit Bureau of Singapore	Credit bureau	Singapore
Credolab	Credit data analytics	Indonesia, Singapore, Vietnam
Dibee	Logistics payments service provider	Vietnam
EFL Lenddo	Data analytics and risk scoring	Global
Experian	Consumer credit reporting and analytics	Global
FE Credit	Consumer finance company	Vietnam
Funding Societies	Person-to-person lending platform	Indonesia, Malaysia, Vietnam
GrowSari	Business-to-business distribution platform for retailers	Philippines
Jumper.ai	E-commerce platform	India, Philippines, Singapore
Myinfo, Govtech	Government digital ID system	Singapore
Refinitiv	Financial market data and infrastructure	Global
Tiaxa	Mobile telco data-analytics firm	Latin America, Southeast Asia
TP Bank	Local retail bank	Vietnam
Truelayer	Banking application programming interface integrator	Australia, Europe
Velotrade	Trade finance platform	Hong Kong, Vietnam
Xero	Cloud-based accounting platform	Australia, New Zealand, Singapore, United Kingdom, United States

B. Relevant Legal and Regulatory Frameworks

Regional:

- APEC Privacy Framework (2015)

Indonesia:

- Law No. 11 of 2008 regarding Electronic Information and Transactions ("**EIT Law**") as amended by Law No. 19 of 2016 regarding the Amendment of EIT Law ("**EIT Law Amendment**")
- Government Regulation No. 71 of 2019 regarding Provisions of Electronic Systems and Transactions ("**Reg. 71**") and its implementing regulation, Minister of Communications and Informatics Regulation No. 20 of 2016 regarding the Protection of Personal Data in an Electronic System ("**MOCI Regulation**")
- Article 40 of Law No. 36 of 1999 regarding Telecommunications ("Telecommunications Law")
- Article 6 of Law No. 14 of 2008 regarding Disclosure of Public Information
- Law 7 of 1992 as amended by Law 10 of 1998 on Banking ("Banking Law") and Law 8 of 1995 on Capital Markets ("Capital Markets Law")
- Financial Services Authority Regulation No. 38/POJK.03/2016 on the Implementation of Risk Management in the Utilization of Information Technology.

Malaysia:

- Malaysia's Personal Data Protection Act of 2010 protects any personal data collected in Malaysia from being misused. According to the act, you must obtain the consent of users before collecting their personal data or sharing it with any third parties. For their consent to be valid, you must give them written notice of the purpose for the data collection, their rights to request or correct their data, what class of third parties will have access to their data and whether they are required to share their data, and the consequences if they do not.
- Credit Reporting Agencies Act, 2010.

The Philippines:

- The Philippines is known for having "**one of the toughest data privacy legislations in the region**." In the Philippines, anyone who collects personal data needs to get specific and informed consent from the user first. You must declare the purpose of the data processing before you begin to collect it (or as soon as reasonably possible after).
- Under the **Republic Act No. 10173**, individuals have the right to know your identity, what personal data you're collecting and for what purpose, how it's being processed, to whom it's being disclosed, and all their rights regarding their own data.
- Credit Information System Act (CISA) of 2008

Singapore:

- Personal Data Protection Act of 2012
- Personal data collection on the basis of consent only
- Individuals must be informed of the purpose for data collection
- Credit Information Sharing Bill (not yet enacted)

Type of Regulation				
Country	**Fintech Regulation**	**Data Protection Law**	**Credit Bureau Law**	**Review of industry by other parties (other than regulators)**
Vietnam	Draft Decree on Fintech Regulatory Sandbox	No single data protection law, but several laws talk about personal data,the key principles on collection, storage, use, process, disclosure or transfer of personal information.	Decree No. 10/2010/ND-CP (On Credit Information Related Activities)	
Source	https://www.indochinecounsel.com/uploa d/news/SpecialAlert_DraftDecreeonFintec hSandbox-forFintech_Oct2020.pdf			
Malaysia	No specific Fintech Act. the Financial Services Act 2013 (FSA); the Islamic Financial Services Act 2013 (IFSA); the Money Services Business Act 2011 (MSBA); the Capital Markets and Services Act 2009 (CMSA); and various standards and guidelines issued by BNM and the SC.	Malaysian Personal Data Protection Act 2010 (PDPA)	Credit Reporting Agencies Act and Personal Data Protection Act 2010	Apart from the regulators, it appears that no other bodies (such as accounting and auditing firms, or other vendors) review and monitor the activities of fintech industry participants. While there are industry associations in Malaysia (such as the Fintech Association of Malaysia), members do not seek to self-regulate the industry and function more as intermediaries between the fintechs and regulators.
Indonesia	Several	No single data protection law, but several laws talk about personal data,the key principles on collection, storage, use, process, disclosure or transfer of personal information.	Bank Indonesia Regulation No.15/1/PBI/2013 Concerning Credit Bureau	
Source			https://www.bi.go.id/en/peraturan/perba nkan/Pages/PBI%20No.15_1_PBI_2013.aspx	
Philippines	lending companies and financing companies organised under the Philippines' Lending Company Act and Financing Company Act, respectively; National Telecommunications Commission (NTC), pursuant to the Philippines' Public	Data Privacy Act 2012	The R.A. No. 9510, otherwise known as the Credit Information System Act (CISA) of 2008	
Singapore	No specific Fintech Act. Captured under different financial services legislation. Has a Fintech Regulatory Sandbox.	PERSONAL DATA PROTECTION ACT 2012	CREDIT BUREAU ACT 2016 (No. 27 of 2016)	
Source		https://sso.agc.gov.sg/Act/PDPA2012	https://sso.agc.gov.sg/Act/CBA2016/Uncom menced/20200930155248?DocDate=2017021 5	

Cambodia	No information	No specific Data Protection Act. Covered through civil code and various industry specific legislation https://www.dataguidance.com/notes/ca mbodia-data-protection-overview#:~:text=Although%20 Cambodia% 20has%20not%20 enacted,entitled%20 to%2 0their%20personal%20rights.	Prakas on Credit Bureau (2733B7-011-145)	
Source		https://www.dataguidance.com/notes/ca mbodia-data-protectionoverview#:~: text=Although%20 Cambodia% 20has%20not%20 enacted,entitled%20 to%2 0their%20personal%20rights.		
Thailand	No specific law. Payments Systems Law. Sandbox under SEC	Personal Data Protection Act ("PDPA"), May 2019	Credit Information Business Acts B.E. 2545, 2549 and 2551 (in 2002, 2006 and 2008	
Myanmar	No information	No information	Regulation on Credit Information Reporting System, March 31, 2017,	
Laos	No information	No information	Decree on Credit Information Bureau	
Brunei	No information	Data Protection Policy Guidance, 2014.	CONSTITUTION OF BRUNEI DARUSSALAM (Order made under Article 8313))	
India	No single act.	Personal Data Protection Bill (forthcoming)	Credit Information Companies (Regulation) Act, 2005 ("CIC Act"),	
Australia	Existing laws and regulations for financial services and consumer credit.	The Federal Privacy Act 1988 (Cth) (Privacy Act) and its Australian Privacy Principles (APPs). State level legislation	Part IIIA of the Privacy Act 1988 (Privacy Act)	
Source	https://www.globallegalinsights.com/pract ice-areas/fintech-laws-and-regulations/australia	DL Piper website		

C. Survey Questionnaire

General Questions
Name of company
Name and position of respondent
Type of organization
Fields of activity
Types of clients
Markets of operation; # thereof
of employees
Years of operations in the region
Is the company licensed or overseen by a financial or consumer/data-protection authority?
Are you part of any association of data analytics/information companies?
As part of your operations, do you collect and analyze data (internally or from 3rd parties) for your own use or for external parties specifically for credit risk assessment, underwriting and monitoring purposes (credit application assessments, credit granting, portfolio mgt, fraud detection, AML, KYC or collections)? - If not, do you intend to use data for the purposes listed above in the future? Own data or third party? - Would you be willing to share own data for these purposes?
Apart from your core business, what percentage of your company's focus (revenues / resources) are directed towards data analytics (collection, analysis and use)?

2	Legal and Regulatory Framework
2.1	a. What are the legal and regulatory requirements for providing data-analytics services? b. Do you need a business registration or license to provide data-analytics services for credit underwriting and credit risk monitoring? c. What are the conditions for licensing or business registration? d. What are the legal and regulatory requirements on using third-party data for credit-underwriting purposes (assessments, KYC, AML, collections, monitoring)? (Qs for DU)
2.2	Does your organization have a dedicated regulation, and compliance function?
2.3	What other laws and regulations govern your activities?
2.4	If regulated, who is the supervisory authority? a. What are the reporting requirements? b. What types of action does the regulator undertake—inspections, audits, on-sites, and so on? c. What are the measures imposed for noncompliance? d. Are the legal and regulatory requirements clear and sufficient? If not, what else needs to be considered? e. Do you have specific regulatory support/reforms to recommend?
2.5	If not regulated, do you follow • Industry/association-driven governance measures? • Codes of Conduct? • Other measures of self-regulation and governance?
2.6	Cross border information sharing • Do the laws and regulations permit cross border information sharing?
2.7	Consent
	• Are there specific legal and regulatory obligations for consumer consent that you follow? In which jurisdictions? • Is consent required? • If yes, how is consent collected? • How long is consent stored for? • Is notification required? If so, how are they notified? • If there is no legal/regulatory requirement for consent, are consumers aware data is collected? • If so, how are consumers notified?

3.	**Business model features**
3.1	(Assuming responded yes to 1.11) How would you differentiate yourself from a credit bureau? a) What additional insights or information do clients get that is not available through other sources? b) Should data-analytics companies be treated different from credit bureaus? Why, why not?
3.2	Do you offer services for retail, commercial or both types of clients?
3.5	Key products and services used, offered (and demanded).
	Credit Risk Assessment? Do you offer credit risk assessment products? If yes, - What types of products? - For internal or external purposes? for external users, what % of revenues is this?
	AML: i. What types of data, databases are consulted? ii. What is the process of conducting AML? Is data stored for AML or accessed per request?
	KYC checks: i. What types of data, databases are consulted? ii. What is the process of conducting KYC? Is data stored for KYC or accessed per request?
	Fraud: i. What types of fraud detection products are offered? ii. What data sources, databases are consulted? iii. What are the processes involved? (for example, identity fraud, credit card fraud, and so on)
	Other services (please indicate service) i. Lead and prospect development ii. Portfolio management, monitoring, analysis iii. Collections iv. Other
3.6	Financial revenue model—please indicate
	a. Membership based with regulation of access b. Subscription-based services on commercial terms c. Fees per use, per user? On demand?
3.7	Clients and Users
	a. Number of clients b. Geographic distribution c. Type of clients: financial institutions, non-bank, utilities, regulators, other? d. Average frequency of use e. What are costs and benefits for clients? f. Are the products you offer used in place of or as a complement to traditional credit bureau reports, scores, and other products?

D. Excerpts from General Principles for Credit Reporting

Data

General Principle 1: Credit-reporting systems should have relevant, accurate, timely and sufficient data—including positive—collected on a systematic basis from all reliable, appropriate and available sources, and should retain this information for a sufficient amount of time.

Data Processing: Security and Efficiency

General Principle 2: Credit-reporting systems should have rigorous standards of security and reliability, and be efficient.

Governance and Risk Management

General Principle 3: The governance arrangements of credit-reporting service providers and data providers should ensure accountability, transparency and effectiveness in managing the risks associated with the business and fair access to the information by users.

Legal and Regulatory Environment

General Principle 4: The overall legal and regulatory framework for credit reporting should be clear, predictable, nondiscriminatory, proportionate and supportive of data subject and consumer rights. The legal and regulatory framework should include effective judicial or extrajudicial dispute resolution mechanisms.

Cross-Border Data Flows

General Principle 5: Cross-border credit data transfers should be facilitated, where appropriate, provided that adequate requirements are in place.

Guidelines on Nondiscrimination

Data supplying and data access should be established in a fair manner, responding to impartial rules regardless of the nature of the participants.

150. Non-discriminatory refers to the legal and regulatory framework being equally applicable to the various participants in credit reporting insofar as they are providing equivalent services. This helps to promote a level playing field that encourages competition on a fair and equitable basis.

151. In principle, all active users of data for lending purposes should be allowed to access credit-reporting databases. A possible exception to this general rule could be the case of some credit registries whose basic purpose is to support banking supervision and improve the availability and quality of credit data for supervised intermediaries—and that as a consequence require data from, and provide access to regulated financial institutions only.

152. In many cases, access to the credit-reporting databases is based on some degree of reciprocity between the data providers/users and the credit-reporting service provider(s). The principles issued by the Steering Committee on Reciprocity may serve as a reference in determining the extent to which reciprocity should be used as the guiding principle with regard to granting access to the credit-reporting databases.

References

[1] See, for instance, World Bank Group and International Committee on Credit Reporting, Credit Scoring Approaches Guidelines (2019), https://thedocs.worldbank.org/en/doc/935891585869698451-0130022020/original/CREDITSCORINGAPPROACHESGUIDELINESFINALWEB.pdf

[2] As defined in International Finance Corporation's Data Analytics and Digital Financial Services Handbook, data is a sample of reality recorded as a measurement and stored as a value. The manner in which data is classified and its format, structure, and source determine which types of tools can be used to analyzed it.

[3] See, for instance, the European Union's recent data policy, https://eur-lex.europa.eu/legal-content/EN/TXT/?qid=1593073685620&uri=CELEX%3A52020DC0066

[4] Recent studies, such as the one by Google, Temasek, and Bain, point to the growing and already important economic size of the digital economy in Southeast Asian markets. The digital lending economy in key markets there is forecast to rise to $92 billion by 2025. See Google, Temasek, and Bain, e-Conomy SEA 2020, https://storage.googleapis.com/gweb-economy-sea.appspot.com/assets/pdf/e-Conomy_SEA_2020_Report.pdf

[5] Survey participants included firms with a global presence and operations in most Southeast Asian markets, as well as firms that were more focused on certain markets in Southeast Asia, including Cambodia, Indonesia, Malaysia, the Philippines, Singapore, and Vietnam.

[6] While there are several different types of data-analytics companies, we are focused only on those that offer services that support the credit-underwriting function in this report.

[7] In most cases, data from firms and data from individual consumers are treated differently. Business firms' data typically has fewer privacy and confidentiality protections because businesses are expected to disclose basic information to the markets to facilitate transactions. At the consumer level, the right to privacy for individuals is a widely held concept that is often reflected in the legislation for credit reporting or in other laws.

[8] The decision to mandate sharing and/or inquiry in any jurisdiction can depend on a number of factors. In markets where credit information sharing is less well understood and there is an inherent lack of trust among lenders, the regulator plays a critical role in building this trust. Mandating the sharing of information enables the credit-information database to be developed, and it also signals to lenders that their peers will also be reporting. Regulators may see value in mandating information sharing and the use of credit information to promote responsible risk-management practices and greater financial stability.

[9] A cell shaded in -dark blue indicates that the market participant is subject to those provisions (through a credit information-sharing framework or other enabling frameworks), whereas a grayed-out cell indicates that market participants are not subject to those provisions.

[10] World Bank, General Principles for Credit Reporting (2011), https://documents.worldbank.org/en/publication/documents-reports/documentdetail/662161468147557554/general-principles-for-credit-reporting

[11] International Committee on Credit Reporting, Use of Alternative Data to Enhance Credit Reporting to Enable Access to Digital Financial Services by Individuals and SMEs Operating in the Informal Economy (June 28, 2018).

[12] It should be noted that many countries have already signaled a shift from using the narrow term banking to finance or to a more general open-data or consumer-data-rights approach.

[13] See https://www.bankofengland.co.uk/-/media/boe/files/fintech/open-data-for-sme-finance.pdf

[14] Refer, for instance, to https://www.w3.org/TR/vc-data-model/#what-is-a-verifiable-credential

[15] The Australian Competition and Consumer Commission has defined a consumer-data-rights regime that applies to multiple sectors, including but not limited to financial services.

16 More recently, Chinese regulators have required Ant Financial to overhaul its businesses (payments, consumer lending, asset management, and insurance) to ensure a more competitive playing field for other fintechs in the market.

17 Examples would include application programming interface integrators that connect different sources of data to enable banks to process applications or specialists in KYC or credit file "enhancement."

18 https://trade.ec.europa.eu/doclib/docs/2021/february/tradoc_159438.pdf

19 OJK (Financial Services Authority of Indonesia) 13/2018. Based on survey responses and http://www.wplaws.com/news/highlight-provision-ojk-regulation-no-13-pojk-02-2018-digital-financial-innovations

20 Law No. 11 of 2008.

21 Law No. 40 of 2007.

22 It should be noted that many e-commerce firms, using transaction data, already take a first-loss risk-sharing approach to lending by financial institutions to merchants on their platform.{-EDIT OK?- Yes OK, IVAN-}

23 It should be noted that this is probably due in part to the sample of firms chosen; many were local to one or two markets. Other views would likely have been expressed had the survey obtained inputs from global platforms such as Amazon or Alibaba.

24 See, for instance, https://www.rieti.go.jp/en/special/policy-update/092.pdf

25 https://www.w3.org/TR/vc-data-model/#what-is-a-verifiable-credential

26 See the recent Financial Stability Institute paper by Juan Carlos Crisanto, Johannes Ehrentraud, and Marcos Fabian, Big Techs in Finance: Regulatory Approaches and Policy Options, FSI Brief No. 12 (Bank for International Settlements, March 2021), https://www.bis.org/fsi/fsibriefs12.pdf

27 These include key observations expressed in a recent study by Coyle and Li on the broader strategic issues in the data economy and trade; see Diane Coyle and Wendy Li, "The Data Economy: Market Size and Global Trade," draft conference version: December 22, 2020.

28 https://www.dlapiperdataprotection.com/index.html?t=enforcement&c=MY

29 The Financial Data and Technology Association (fdata) is one association that regroups a cross-section of firms involved in open finance.

30 Coyle and Li, "The Data Economy."

31 https://www.bankofengland.co.uk/-/media/boe/files/fintech/open-data-for-sme-finance.pdf?la=en&hash=FD4BC43BBD61EDEC5F8460C6BB7488EFDE647581

32 See https://consultation.accc.gov.au/communications-1/consumer-data-right-rules-framework-consultation/supporting_documents/ACCCConsumerDataRightRulesFramework.pdf

33 A model is explainable when its internal behavior can be directly understood by humans (interpretability) or when explanations (justifications) can be provided for the main factors that led to its output. The significance of explainability is greater whenever decisions have a direct impact on customers/humans, and it depends on the particular context and the level of automation (artificial intelligence/machine learning) involved. Lack of explainability could represent a risk in the case of models developed by external third parties and then sold as opaque packages. Explainability is just one element of transparency. Transparency consists of making data, features, algorithms, and training methods available for external inspection and constitutes a basis for building trustworthy models.

34 Peter Carroll and Saba Rehmani, Point of View: Alternative Data and the Unbanked (Oliver Wyman, 2017), https://www.oliverwyman.com/content/dam/oliver-wyman/v2/publications/2017/may/Oliver_Wyman_Alternative_Data.pdf.

35 https://www.economist.com/briefing/2017/05/06/data-is-giving-rise-to-a-new-economy

36 https://www.economist.com/special-report/2020/02/20/are-data-more-like-oil-or-sunlight

IFC | International
Finance Corporation
WORLD BANK GROUP