RESPONSIBLE USE OF TECHNOLOGY IN CREDIT REPORTING

White Paper

WORLD BANK GROUP

ICCR
INTERNATIONAL COMMITTEE ON CREDIT REPORTING

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

Table of Contents

Executive Summary **6**

Introduction **8**

Use of Technology in Credit Reporting **10**
2.1. Disruptive Technologies in Credit Reporting 11
2.1.1. Smartphones 11
2.1.2. Digital Payments 11
2.1.3. Big Data 11
2.1.4. Open Banking 12
2.1.5. AI/ML 13
2.1.6. Digital ID & Biometrics 14
2.1.7. Cloud Computing 14
2.1.8. Distributed Ledger Technologies 14
2.2. Implications of Innovations in Credit Reporting 15
2.2.1. Benefits and Opportunities 15
2.2.2. The Emergence of Alternative Credit Reporting Service Providers 16
2.2.3. Risks and Challenges 17

Stocktake and Analysis of Responsible Use of Technology Frameworks **20**
3.1. Ethics and Human Rights for Responsible Use 20
3.2. Big Data 21
3.3. Open Banking & Open APIs 21
3.4. AI/ML 22
3.5. Digital ID & Biometrics 23
3.6. Cloud Computing 23
3.7. Distributed Ledger Technologies 23

Principles for the Responsible Use of Technology in Credit Reporting **26**
4.1. Principle 1: Fairness 27
4.2. Principle 2: Ethics 27
4.3. Principle 3: Accountability 27
4.4. Principle 4: Transparency 28
4.5. Principle 5: Security and Robustness 29
4.6. Principle 6: Lawfulness 29
4.7. Principle 7: Privacy 29
4.8. Principle 8: Sustainability and Well-Being 29
4.9. Principle 9: Inclusivity 30
4.10. Principle 10: Trust 30

Considerations for Implementing the Principles **32**
5.1. Applying the Principles 32
5.2. Capacity Building 33
5.3. Technology-Specific Recommendations 33
5.4. Use Cases 34

Appendix A **36**
Appendix B **40**
Appendix C **42**

Abbreviations

AI	Artificial intelligence
AISP	Account information service provider
API	Application program interface
BCBS	Basel Committee on Banking Supervision
BIS	Bank for International Settlements
CRSP	Credit reporting service provider
CSP	Cloud service provider
DLT	Distributed ledger technology
EBA	European Banking Authority
EU	European Union
FCRA	Fair Credit Reporting Act
Fintech	Technology-enabled financial services
FSB	Financial Stability Board
GDPR	General Data Protection Regulation
ICCR	International Committee on Credit Reporting
ID	Identification
IEEE	Institute of Electrical and Electronics Engineers
IOSCO	International Organization of Securities Commissions
ISO	International Standards Organization
ITU	International Telecommunications Union
LEI	Legal Entity Identifier
MAS	Monetary Authority of Singapore
ML	Machine learning
MSME	Micro small and medium enterprise
OECD	Organization for Economic Co-operation and Development
PBOC	People's Bank of China
P2P	Peer to peer
SME	Small and medium enterprise
TPP	Third-party provider
UN	United Nations
UNDG	United Nations Development Group
UNESCO	United Nations Educational, Scientific & Cultural Organization
WAEMU	West African Economic and Monetary Union
WEF	World Economic Forum

Acknowledgements

This paper is a product of the International Committee on Credit Reporting (ICCR) and the World Bank Group. The paper was prepared by Talha Ocal and Dilip Santlani (independent consultants) under the leadership and guidance of Collen Masunda, Secretariat of the ICCR, and the ICCR Communications and Knowledge Management Working Group, chaired by Giovanna Cardellicchio (Alacred).

The document benefited from a consultation process and the contributions of plenary members, representative organizations, and external peer reviewers. The committee gratefully acknowledges valuable inputs and comments from peer reviewers Natalia Bailey (Research Manager, FinRegLab) and Dr. Michael Akinwumi (Chief Tech Equity Officer, National Fair Housing Alliance).

The ICCR would also like to thank the Chairman of the ICCR, Mahesh Uttamchandani, and Secretariat members Luz Maria Salamina and Collen Masunda for guiding the process. Susan Boulanger provided editorial services. The layout and design of the report was prepared by Nitin Kapoor.

Chapter

Executive Summary

Technology is at the core of credit reporting systems, which have evolved significantly over the past decade by adopting new technologies and business models. Disruptive technologies such as advanced computing, artificial intelligence (AI), machine learning (ML), big data analytics, and digital payments are reshaping the credit reporting industry. Innovations have enabled credit reporting service providers (CRSPs) greater access to and sharing of data with improved analytics capabilities. As a result, the population coverage of credit reports increased, the scope of processed data expanded, and credit reports were delivered much faster.

As disruptive technologies have been increasingly adopted around the globe, concerns have arisen over possible misuse or unethical use of these new technologies. These concerns inspired international institutions and national authorities to issue high-level principles and guidance documents on responsible technology use. While adopting new technologies benefits the credit reporting industry, unintended negative outcomes of these technologies from ethics and human-rights perspectives must also be considered. Against this background, ICCR is pleased to offer this white paper as a framework for responsible use of technology in credit reporting activities.

The white paper begins with a brief introductory section, followed in Section 2 with a discussion of technology use in credit reporting, with a special focus on the key disruptive technologies being increasingly adopted by the industry. In parallel with innovation, the role of credit reporting has also evolved, and CRSPs are transforming into technology-intensive entities that provide a wide range of data analytics solutions beyond credit reporting. Moreover, the explosion of technological advancements has led to the emergence of alternative credit reporting service providers in the industry. The section also discusses the implications of new technologies from the dual perspective of benefits and opportunities and risks and challenges.

Section 3 provides information on the scope, development, and high-level principles of several key technology frameworks, including the principles underlying their responsible use. The selection of frameworks for this section was made using criteria such as global applicability, relevance to the credit reporting industry, and suitability from the perspective of responsible use.

Section 4 introduces ten principles to guide responsible use of technology in credit reporting activities. By applying these principles, the industry can make the best, most responsible use of disruptive technologies while benefiting all stakeholders. To ensure this objective, the principles are technology agnostic and apply to all types of technologies used in credit reporting activities. Participants in credit reporting systems are expected to apply these principles proportionately, according to their technology use. The principles are not mutually exclusive; each entity using technology-supported credit reporting systems should apply them in totality.

The principles are as follows:

1. **Fairness.** Credit reporting systems should ensure the fair use of technologies deployed in their operations. Technology-driven credit reporting products should at all times protect the fundamental rights of individuals and should not discriminate against any individuals, groups of consumers, or SMEs.
2. **Ethics.** Credit reporting system participants should ensure that any technology they adopt and use complies with their corporate values, codes of conduct, and highest ethical standards. Technology-driven decisions should be held to at least the same ethical standards as human-driven decisions.
3. **Accountability.** Credit reporting system participants are accountable for the use of both internally developed and externally resourced technologies. Appropriate governance mechanisms should be in place to oversee the processes of technology-driven credit reporting products.
4. **Transparency.** Credit reporting system participants should ensure that the techniques and methods used in their technology-driven decisions are explainable, assessable, and understandable by relevant stakeholders.
5. **Security and Robustness.** Credit reporting systems should be governed by an appropriate data security

framework to ensure the confidentiality, integrity, and availability of information at all times. The robustness of technologies should be ensured to avoid unintentional harm to individuals.

6. **Lawfulness.** Credit reporting system participants should ensure that the use of data and technologies is lawful and complies with relevant regulations and professional standards.
7. **Privacy.** Credit reporting system participants should protect the privacy of data subjects while accessing, collecting, analyzing, processing, and distributing their data for credit reporting.
8. **Sustainability and Well-Being.** Technologies employed in credit reporting systems should support human well-being and be sustainable in all human, social, cultural, economic, and environmental aspects.
9. **Inclusivity.** The adoption and use of technological innovations in credit reporting systems must not result in or accentuate the exclusion of any individual or group of individuals.
10. **Trust.** Technologies employed in credit reporting systems should be considered trustworthy in the eyes of stakeholders, including data subjects and financial institutions.

Finally, Section 5 discusses considerations for applying the principles. It discusses how to assess a technology for possible use, highlights the need for capacity building, and provides additional technology-specific recommendations to guide adopters. The section concludes with use cases illustrating the principles in action.

Chapter 1

Introduction

Over the past decade, technological advancements and innovations, including advanced computing, artificial intelligence (AI), and machine learning (ML), have exploded, reshaping the credit reporting industry. These innovations enable greater access to data (big data), and data sharing takes place with better identification, transaction, networking, analytics, and other capabilities, significantly impacting the industry. Improved algorithms also play a more significant role in credit risk management and promote access to credit for unserved and underserved communities. By opening doors to the use in credit decision-making of nontraditional data sources, such as rental, telecommunication, and cash flow data, these technological advancements allow individuals or businesses previously unscorable or invisible under mainstream credit systems to gain access to credit.

Technologies are accelerating the evolution of regulatory standards as well as providing tools to oversee regulatory compliance. Regulatory authorities leverage these technological enhancements to improve their oversight and policy development functions. For example, advanced computing and analytics enable regulators to access and use broader data sets for policy making and supervision. The technologies also allow regulatory bodies to automate the supervisory processes to some extent with the help of the RegTech and SupTech tools being developed by emerging tech startups.

Yet the spread of new technology and disruptive changes in the credit reporting ecosystem raises concerns about possible unintended negative consequences. For example, use of AI/ML and big data analytics has raised several questions regarding the transparency of the processes, the privacy of the data being accessed, and potential biases internalized into the algorithms and models. Other concerns relate to lack of clarity over how well these new technologies fit into and comply with existing regulations. For example, big data acquisition and processing, use of cloud computing, reliance on third-party vendors and the black boxes associated with AI/ML systems can be contrary to regulations. Further, some of these technologies might raise privacy and security concerns, including data ownership and confidentiality issues.

While adopting new technologies benefits the credit reporting industry, their implications from the ethics and human-rights perspectives must also be considered. International institutions, national regulatory agencies, and industry associations thus have issued guidance and directives on responsible use of technology, but the effort remains in its infancy, and little material guidance directly applies to the credit reporting industry. In most cases, the guidance documents focus on ethical use of AI/ML.

Against this background, this white paper aims to present for consideration by credit reporting industry stakeholders a framework that combines ethics and rights-based approaches to responsible technology use. The paper begins by reviewing the use of new technologies in credit reporting and then evaluates the rights and ethics frameworks that apply to such use and proposes principles for responsible technology use in credit reporting going forward. Finally, the document discusses how the proposed responsible use principles can be instituted. Applying the proposed principles as appropriate will facilitate the credit reporting industry's best most responsible use of disruptive technologies to the benefit of all stakeholders.

17-06-03T18:42:18.018", "deltaStartMillis":"e
manager.handlers.RequestHandler", "method":"handle",
", "message":"Duration Log", "durationMillis":"508"}{
ge/analyze", "webParams":"null", "class":"com.orgmanag
68e-afd8-46ac-9745-839146a20f09", "sessionID":"144o2n6
"36"}{"timestamp":"2017-06-03T18:43:335.030","deltaSta
=chartdata_new.json", "class":"com.orgmanager.handlers
2n620jm9trnd3s3n7wg0k", "sizeChars":"48455", "message"
":"0", "level":"INFO", "webURL":"/app/page/report", "w
89cb-bfa8-4e7d-8047-498454af885d", "sessionID":"144o2n
"7"}{"timestamp":"2017-06-03T18:46:921.000", "deltaSta
nager.handlers.RequestHandler", "method":"handle", "m
", "message":"Duration Log", "durationMillis":"10"}{"
t/json/file", "webParams":"file=chartdata_new.json",
e95-19e2-4a60-88d7-6ead86e273d1", "sessionID":"144o2n
23"}{"timestamp":"2017-06-03T18:42:18.018", "deltaSta
nager.handlers.RequestHandler", "method":"handle", "m
, "message":"Duration Log", "durationMillis":"508"}{"
e/analyze", "webParams":"null", "class":"com.orgmanag
8e-afd8-46ac-9745-839146a20f09", "sessionID":"144o2n6
36"}{"timestamp":"2017-06-03T18:43:335.030","deltaSta
chartdata_new.json", "class":"com.orgmanager.handlers
n620jm9trnd3s3n7wg0k", "sizeChars":"48455", "message"
:"0", "level":"INFO", "webURL":"/app/page/report", "w
9cb-bfa8-4e7d-8047-498454af885d", "sessionID":"144o2n
7"}{"timestamp":"2017-06-03T18:46:921.000", "deltaSta
nager.handlers.RequestHandler", "method":"handle",

Chapter 2

Use of Technology in Credit Reporting

Technology is at the core of credit reporting systems. From the era of paper-based credit reports to today's automated lending systems, credit reporting service providers (CRSP) have adopted technological advances to update and improve their capabilities in creating and delivering credit reports. In parallel with innovation, the role of credit reporting has evolved, and CRSPs are transforming into technology-intensive entities that provide a wide range of data analytics solutions (Figure 1).

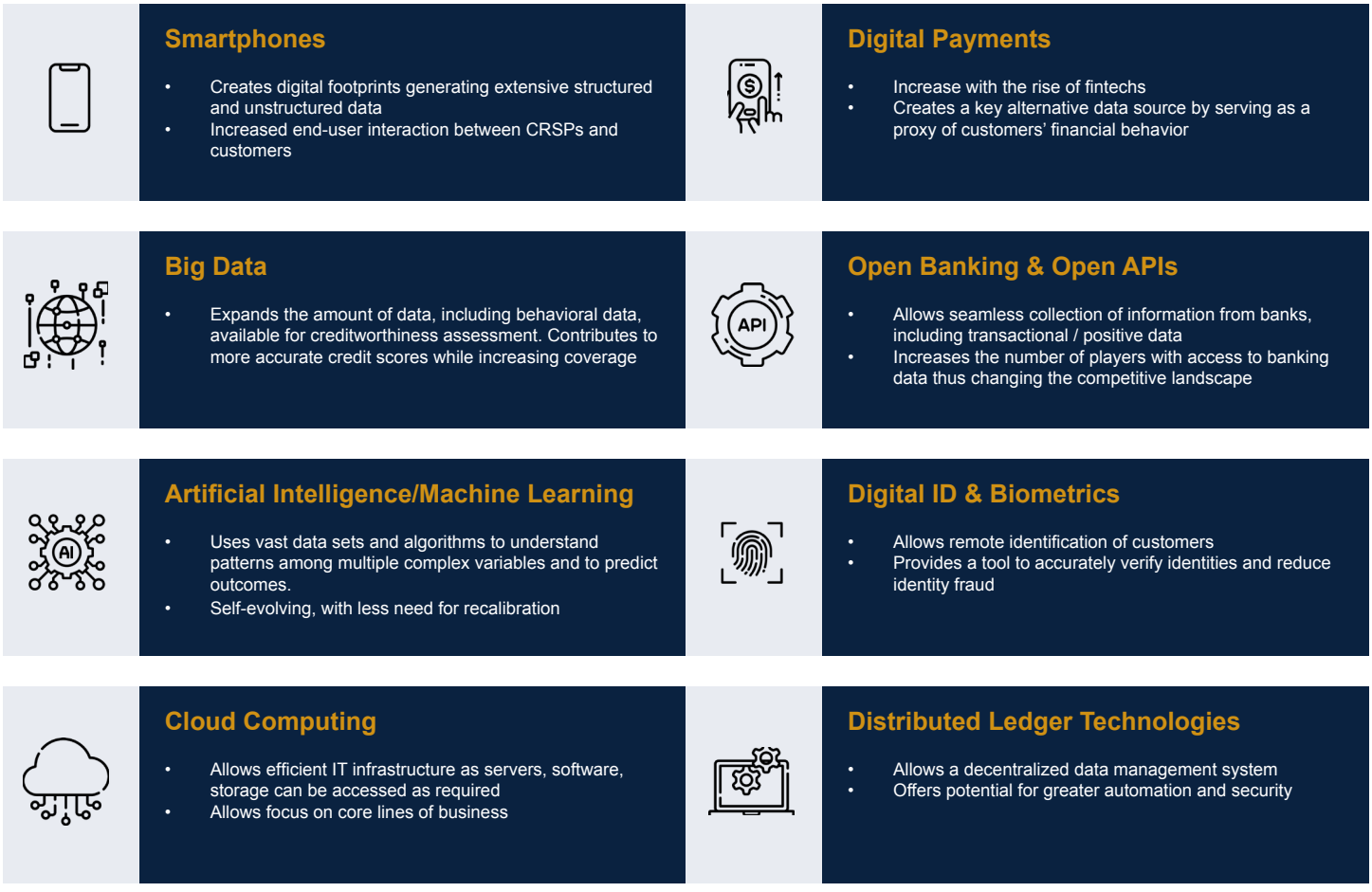

Figure 1: Innovations Affecting the Credit Reporting Industry (Source: Authors).

2.1. Disruptive Technologies in Credit Reporting

2.1.1. Smartphones

Credit reporting systems have room to improve their coverage of the global population. A large population cannot access traditional financing channels due to insufficient prior credit history. In the top 20 economies, 83 percent of the adult population on average is covered by a credit bureau or registry, whereas in the bottom 50 economies the average coverage is only at 10 percent (World Bank 2020). Due to the telecommunication revolution, however, a majority of the global population has access to some form of mobile device. As of October 2021, there were 5.29 billion unique mobile phone users (67.1% of the population) globally and 4.44 billion mobile internet users. Of the mobile internet users, 89.6 percent used smartphones (Data Reportal 2021).

Over the years, smartphones have transformed into a one-stop platform for most activities. Thus, mobile devices generate a large quantity of both structured and unstructured data through the general use of the device itself. Examples of structured data are transactional data, such as top-up patterns, utility payments, and mobile money use; unstructured data include details of the consumer's use of these devices, such as browsing patterns and social media footprints. While structured data based on transactions has more descriptive value for CRSPs, unstructured data also holds value, allowing CRSPs to assess borrowers with inadequate transactional data.

These nontraditional data sources are valuable for credit reporting because, first, they can capture comprehensive details on individuals, which when coupled with other data sources can create a credit report on the user. Second, CRSPs can use the data to assess individuals who have had no exposure to the traditional credit services. Smartphones thus provide a valuable tool for assessing the creditworthiness of consumers who lack formal relationships with a financial institution. In some cases, these sources offer the only data available on a consumer's or SME's behavior. Without such information credit risk is very difficult to measure, leading the financial institution to deny credit or charge excessively high costs. Evidence from modeling shows that performance based on credit score and digital footprint variables significantly exceeds performance based on either credit score or digital footprint variables alone (Berg et al. 2019). As a result, many CRSPs have adopted nontraditional data generated through smartphones for credit scores and developed applications for consumers to monitor their credit scores. For example, Experian in India partnered with First Principle Labs to develop a mobile app that helps consumers access their credit scores free of cost and provides personalized tips on improving credit scores.

2.1.2. Digital Payments

As a result of the accelerated rise of electronic commerce and online shopping channels, digital payment platforms are extensively used by growing numbers of consumer. These platforms address the limitations of cash payments and provide fast, convenient, safe transactions for both individuals and businesses. Digital payment platforms include electronic funds transfer instruments, digital payment cards, and e-money instruments. In addition, the adoption of digital payments creates large amounts of transactional and cashflow data for both payers and payment acceptors, which can be used for behavioral analysis, debt estimation, income estimation, and forecasting cash flows. Especially for developing markets, digital payments data has expanded credit reporting system coverage to individuals and SMEs previously were unable to access finance.

Electronic and mobile payments platforms have emerged as a significant source of alternative data for use in credit reporting systems, and their coverage accelerated during the COVID-19 pandemic. E-commerce giants take advantage of transactions data to evaluate the creditworthiness of their sellers and customers. E-commerce platforms often come with financing options. For example, Amazon Lending uses the proprietary data of small businesses that sell through the Amazon marketplace. It offers loans to sellers directly or via third-party lenders. M-Shwari in Kenya offers deposits and loans to its customers through its M-Pesa mobile money system, using M-Pesa payments and phone data to determine credit scores. Unlike Amazon Lending, M-Shwari reports its clients to the credit bureau.

2.1.3. Big Data

While credit reporting still mainly relies on traditional data sources, big data is increasingly used. The attributes used to qualify a dataset as big data are volume, velocity, variety, veracity, and value, and innovative technologies are the quintessential tools for leveraging insights from these dimensions of big data. In addition, big data require these innovative technologies to extract outcomes of predictive value to support creditworthiness assessments. The growing number of digital devices, internet-of-things (IoT) devices, and other technological innovations have increased the amount of data generated on various platforms. Reliable sources of nontraditional data have several common attributes. Among them are: (i) coverage of an adequate number of consumers, (ii) compliance with regulations for data privacy, security, and protection, (iii) relevance and predictive power, (iv) ability to enhance already existing traditional data, (v) ability to provide accurate, up to date, and timely information, and (vi) links to a specific individual (ICCR 2018). As a result, CRSPs increasingly use alternative data sources to support their creditworthiness

assessments. Adopting alternative data in credit reporting systems can promote access to creditors for individuals and MSMEs with little or no credit history. In addition, studies support that alternative data have explanatory power in predicting default probability and complementing, rather than substituting for, traditional data when analyzing creditworthiness (Berg et al. 2019). As such, globally active CRSPs have been looking for ways to leverage alternative data sources to expand their coverage.

TransUnion's CreditVision Link leverages alternative sources of data to evaluate consumers' payment behaviors and transactional activities. It provides a tool for analyzing consumer behavior over time to help shape tailored products offered by lenders.

TransUnion acquired FactorTrust, which specializes in nonprime consumers, to provide predictive credit data, analytics, and risk scoring solutions.

Experian Boost allows consumers to add additional on-time payments to their credit reports by linking their bank accounts. Payments made to qualifying utility, cell-phone, and video streaming platforms can be connected to the users' accounts, boosting their credit scores.

Equifax-owned DataX uses alternative payment transactions (e.g., checks, cash, or money orders) to create comprehensive credit reports.

Creditinfo-owned Coremetrix leverages psychometric data collected via online applications to generate credit scores for consumers with thin credit files.

Box 1: Examples of CRSPs' Expanding Coverage

The new digital era has also led to the emergence of super apps that serve as single portals to a wide range of products and services. These services include mobile payments, e-money transfers, payment installments, e-commerce credits, and digital loans. Super apps leverage a wealth of data, including extensive transaction data. This data is often processed to develop credit scores by leveraging AI/ML-based models, so the super apps can offer consumers financial products on their platforms. Depending on the information the super apps collect, they can give lenders an information advantage in credit scoring relative to a traditional credit bureau (Frost et al. 2019). Prominent super app platforms include WeChat and Alipay in China, Go-Jek and Grab in Southeast Asia, and Mercado Libre in Latin America, to name a few. In essence, these BigTech platforms have been transformed into alternative lenders in their regions, developing their credit scoring models by leveraging AI and using alternative data, and may not be part of the credit reporting systems in the countries they operate.

2.1.4. Open Banking

Open banking interfaces allow third-party providers to access information at banks and then develop innovative products based on it. These providers, licensed in the European Union (EU) as account information service providers (AISP), can securely connect to the banking systems using application programming interfaces (API) that hold certain specifications. APIs improve the efficiency, quality, and accuracy of data collection from banks and enable the seamless extraction of transactional data to produce credit scores. Thus, data available via open banking is not limited to narrow indicators such as credit balances or loan arrears. Open banking provides an effective tool for CRSPs to collect data from banks and expand the scope of credit reporting information, while enabling fintechs to collect and process information from banks, which can then be leveraged to develop credit scores (Box 2).

Equifax acquired the open banking fintech AccountScore in the UK to enhance its data analytics capabilities.

TransUnion offers an integrated service using open banking APIs to access transactional bank account information to assist customers with creditworthiness and affordability assessments.

CRIF acquired the open banking fintech Strands, which offers AI-based personal financial management tools.

Bonify in Germany uses transactional data from open banking platforms to create credit scores based on historical and current transactional data.

Quod, based in Brazil, uses positive transactional data from consumers to provide ML-powered credit scores. Since its approval, positive data has driven delinquency rates down and broadened access to credit for both consumers and firms.

Based in France, Algoan leverages open banking data to provide credit decisioning services. As France follows a "negative" credit reporting approach, open banking can play a key complementary role by providing positive payment behavior data.

Box 2: Examples of the Use of Open Banking for Credit Reporting

Likewise, open data initiatives are encouraged by countries such as the UK and New Zealand to foster competition and innovation. These public or private initiatives provide freely available data, usually accessible by APIs, to promote open-source technologies and leverage big data. Open data platforms can be reliable sources of traditional and alternative data for CRSPs, provided that security, integrity, and quality conditions are met. However, open

data is not without risks. These platforms raise concerns on cybersecurity, fraud, and the ethical use of data. Notwithstanding the potential benefits to CRSPs, open data brings challenges to the credit reporting industry. Fintechs can leverage an extensive amount of data at once to develop credit scores and emerge as competitors to CRSPs.

2.1.5. AI/ML

Artificial intelligence (AI) generally refers to technologies that enable problem-solving by allowing computers to think, understand, and learn. AI enables computers to learn, understand, or think so that they can either do things that at present humans can do better or do things that require massive labor or human time. In essence, AI is the practice of adding human capabilities to machines. CRSPs use AI to offer various products, including, but not limited to, credit scoring models, fraud detection, and personal financial management. Machine learning (ML) is a subset of AI that analyzes patterns in big data from diverse sources and produces reliable outputs. An ML-capable machine or computer can learn from patterns without being explicitly programmed to do so. ML is the type of AI most used for credit decisioning, product recommendations, hiring decisions, and market segmentation (ICCR 2019a).

Traditional forms of automated prediction also use computers to make computations, but they typically rely on programmers to define the basic relationship between the inputs and the target variable. ML algorithms are usually given only the target variable, which is then used in computationally intensive processes to identify relationships between various data inputs and the target variable and produce a predictive model. The ML algorithm thus has the capacity to change computational processes and improve the model's performance at each step of the process.

ML can find patterns for credit scoring in nontraditional and unstructured data that traditional statistical models find either impossible or difficult to detect. Thus, ML expands the range of information that can be leveraged to assess creditworthiness. As a result, ML models are increasingly used for credit scoring (Figure 2).

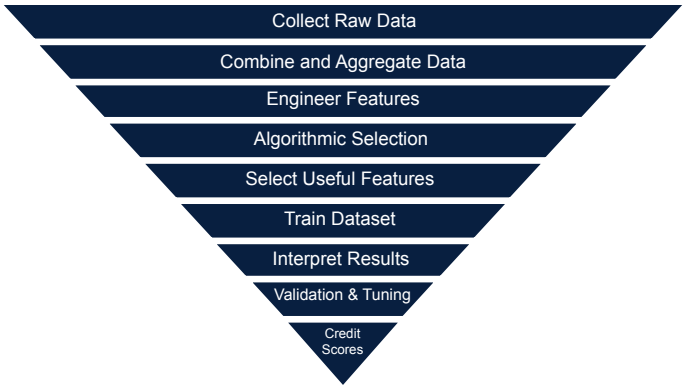

Figure 2: ML Steps for Credit Scoring (ICCR 2019a)

Studies support the idea that AI/ML-based credit scoring models can outperform basic statistical models and that nontraditional data improves an ML-based model (Gambacorta et al. 2019). AI/ML techniques add particular value for predicting the creditworthiness of consumers and businesses with thin credit files. While AI can promote financial inclusion, it involves algorithmic processes for decision-making that are often difficult to interpret or explain. In addition, AI models sometimes use proprietary algorithms. Their decision-making processes are protected as trade secrets, which makes third-party assessments of these algorithms more difficult, as opposed to traditional models.

Explainability is fundamental to understanding and validating the internal behavior of AI/ML systems. Explainability in general refers to the ability to understand the high-level decision-making processes used by a model, and it is relevant to evaluating the model's overall behavior and fitness for use. Explainability also refers to the ability to identify the basis for individual decisions directed by the model. ML algorithms have a varying degree of intrinsic explainability or interpretability, and in most cases, they behave as black box models. Techniques can be used to help understand AI/ML models despite the opacity of their underlying algorithms (CSSF 2018). While the industry standard uses logistic regression models for credit scoring, CRSPs are working to develop AI/ML models that will satisfy jurisdictions' concerns and comply with existing and expected regulations (Box 3).

Equifax developed a NeuroDecision model that aims to comply with US regulations requiring disclosure of reasons for an adverse decision on a loan application. The model provides users with logical and actionable reason codes (Equifax 2020a).

TransUnion has deployed a flexible framework into its ML model development and production scoring processes that enhances explainability while maintaining predictive power, including path-based tree explainability methods, conditional expectations-based Shapley values, and other model diagnostics and feature attribution techniques.

Trackstar.ai, based in the US, uses historical dispute data to develop a prediction model. Its model claims to leverage explainable AI techniques so that solutions can be analyzed and understood by humans.

Studies also support the technical possibility of building explainable AI models for credit scoring (Bussmann et al. 2021).

Box 3: Efforts Toward Explainable AI

2.1.6. Digital ID & Biometrics

An essential step in producing credit reports is to accurately match and merge data subjects' identities from various sources of information. Basic identification (ID) data such as names, addresses, and birth dates can be missing in the collected data, especially in developing countries. In some instances, public ID systems may have multiple enumerations. As of 2018, it is estimated that one billion people worldwide do not have essential identity documents (World Bank 2021b). Creating unique IDs for individuals also plays a special role in helping unserved and underserved populations access finance. Accurate identification is also important for business credit reports. In many cases, standard identification data such as a taxpayer ID or business ID is not available or reliable for businesses. CRSPs often use algorithms to analyze data for the unique identification of businesses. As a global initiative, the Financial Stability Board (FSB) created the Global Legal Entity Identifier Foundation to facilitate worldwide adoption of unique Legal Entity Identifiers (LEIs). Some credit registries (as in Germany and Spain) use LEIs to identify businesses, but their use by CRSPs is globally low (World Bank 2018).

From an innovation perspective, algorithms' improved ability to match pieces of ID-related information and collate them under unique IDs plays a key role in producing accurate credit reports. Biometric tools are used in credit reporting for ID verification through unique physical or behavioral characteristics. Physical (e.g., fingerprints, facial recognition, voice recognition) and behavioral (e.g., typing dynamics, location behavior) characteristics of an individual can be extracted for the purpose of biometric recognition. Wide adoption of smart devices capable of biometric recognition has also been a principal driver in this field. In addition, the COVID-19 pandemic accelerated use of biometric ID verification as an efficient tool to protect against identity fraud while enabling seamless digital onboarding of customers. To this end, CRSPs offer products to properly authenticate and verify identities and help prevent identity fraud.

2.1.7. Cloud Computing

Cloud computing technologies offer a wide range of on-demand services over the internet, including IT resources such as servers, software, storage, databases, etc. Because the services are offered on-demand, they eliminate the large setup costs and initial investments that had been barriers for businesses. Three of the service models available are SaaS (software as a service), IaaS (infrastructure as a service), and PaaS (platform as a service).

Cloud computing technologies use remote server networks for data processing and optimize performance by taking advantage of unused processor capacity. Financial institutions increasingly implement cloud computing with a cloud-first approach that complements legacy IT infrastructures. Not surprisingly, most fintechs adopt a cloud-only or cloud-native approach. Legacy IT infrastructures are still used in the credit reporting industry, but cloud computing is increasingly taking over and is expected to become standard practice for CRSPs (Box 4).

After the industry's most significant data breach, Equifax adopted a cloud-native transformation strategy for its credit reporting services (Equifax 2020b).

TransUnion implemented a hybrid multi-cloud strategy and shifted its on-premise technology to cloud infrastructure.

Experian built a cloud-based sandbox environment that feasibly enables credit score modeling using large amounts of data.

Creditinfo leveraged a SaaS solution to develop a regional hub and spoke credit information-sharing system in WAEMU countries. [1]

Box 4: Examples of CRSPs' Use of Cloud Computing

Cloud services promote a convenient shift to distance working, as seen during the COVID-19 pandemic, ensuring business continuity and operational resilience under severe conditions. Yet cloud computing can facilitate cross-border services in hub and spoke credit reporting infrastructures that serve multiple markets and enable regional integration. Although CRSPs have adopted or are looking to adopt cloud computing, switching to cloud-based services can be challenging. Integrating cloud services with legacy IT systems requires a sound cyber-governance strategy. Also, in many jurisdictions, data sovereignty legislation restricts or prohibits transferring, storing, and processing data at remote cloud servers based outside national borders. For example, when personal data of an EU resident is processed, the CRSP must comply with General Data Protection Regulation (GDPR) requirements, even if it does not directly operate in any EU jurisdiction.

2.1.8. Distributed Ledger Technologies

Distributed ledger technologies (DLT) allow data to be recorded, accessed, and shared across a distributed network of different participants. A "blockchain" can be used in distributed ledgers to store and transmit data in encrypted packages called blocks that are connected in a digital chain. Blockchain immutably records transactions of members of a shared network without any intermediary. DLT and blockchain technologies have the potential to introduce a greater level of automation, security, and privacy control for processing data and to disrupt the way information is shared.

While innovation advocates suggest blockchain technology can transform the industry (Gohardashy et al. 2018), key challenges exist for enabling a full-scale blockchain-based transformation for credit reporting. These challenges include the scalability of IT infrastructures, ensuring data privacy, and complying with data retention periods (Liu and Hou 2021). Fintechs, CRSPs, and especially alternative credit reporting service providers are exploring ways to use DLT and blockchain to collect and share credit information securely and effectively (Box 5).

US-based startup Bloom developed a decentralized, blockchain-based digital ID platform and partnered with TransUnion to offer free credit scores.

Kiva launched Africa's first national decentralized ID system with Hyperledger Indy to issue digital ID to all citizens of Sierra Leone. As a country with over 80 percent of the population unbanked, the open-source blockchain technology provides a fast, secure, free way for the unbanked to open a savings account and move into the formally banked population.

The People's Bank of China (PBOC) is working on using blockchain to share the credit information of regional CRSPs, providing a secure and efficient way to aggregate information currently available only in isolated data islands (Source: PBOC).

Box 5: Examples of DLT Use in Credit Reporting

Another use of DLTs is in cryptocurrencies. Using DLT or centralized ledgers, cryptocurrencies surfaced as a digital currency alternative. Bitcoin, Ethereum, and others use online ledgers with strong cryptography to secure online transactions. Used more and more widely, cryptocurrencies are often traded without regulatory oversight by any jurisdiction. Notwithstanding the risks, cryptocurrencies are potential sources of alternative data not used by many CRSPs.

2.2. Implications of Innovations in Credit Reporting

The credit reporting ecosystem has evolved significantly in the past decade by adopting new technologies and business models. As a result, the accuracy, depth, and breadth of credit data has been improved. Delivery of credit reports is much faster, if not instant. Despite the benefits, improved technologies represent a source of risk for credit reporting systems, such as strategic, operational, cyber, and compliance risks (BCBS 2019). These risks are in addition to those traditionally associated with credit reporting activities. Hence, CRSPs that adopt and leverage advanced technologies should ensure that their IT and other risk management processes and control environments can effectively address new sources of risk.

2.2.1. Benefits and Opportunities

Big data analytics improves financial inclusion by increasing the data sources used to build credit scores for customer segments with little or no formal financial borrowing history, expanding the reach of lending institutions to otherwise underserved customers. To the extent a customer's digital footprint enables creditworthiness assessments as reliable as those from traditional data sources, mainstream adoption of big data for credit scoring has strong implications for expanding access to credit.

The use of big data analytics has also paved the way for creating hyper-personalized services, because lenders can analyze customers' spending patterns and provide customized offerings to better suit their needs. Behavioral analysis of customers enables creditors to price loans accordingly. Digital payments also permit customized collections, such as variable repayment based on revenues, thus improving the management of credit risk.

Open APIs (application program interfaces) provide readily available and reliable real-time information support for CRSPs, reducing the need for data validation, eliminating potential human errors that happen during manual check-ups, and speeding up processing of consumers' transactions data. Further, by connecting other APIs, CRSPs can improve their insights into customer behavior and offer personalized services. A further benefit is the potential for enhanced collaboration among financial institutions and CRSPs to better meet customers' expectations. Over time as more third parties use APIs, the interfaces mature through multiple cycles of fixing issues found in various iterations. APIs help to scale as multiple partners can use the same API to process transactions data. Every iteration using APIs further matures the open banking ecosystem and increases trust in API use.

AI/ML methods allow greater flexibility in analyzing data, often in volumes and at speeds and levels of complexity well beyond what humans can achieve. AI/ML models can improve the ability to infer the entire distribution of potential outcomes and understand the variability of model predictions, which can translate into stronger credit risk management tools. AI/ML can also capture historical fraud patterns and recognize similarities in chains of events before a fraud takes place. They can anticipate and detect fraudulent transactions, cyber-attacks, and related risks. AI/ML can be used to entirely automate lending decisions without need for human involvement. For example, Experian's Ascend Intelligence Services provides a lending platform with AI-based decision models and strategies to help automate credit-granting decisions.

Biometrics is a proven, reliable way to authenticate identities and is the method most resistant to counterfeiting

and spoofing, though it can be abused if oversight is lacking. Biometrics automates and smooths customer identification and verification processes hassle-free for the credit reporting industry and hence serves as a valuable solution for regulatory know-your-customer requirements. Digital ID technologies also enable CRSPs to verify customers' identities rapidly and cost-effectively. In addition, it can provide real-time credit reporting services with fewer concerns about identity theft and similar impersonation-related threats.

Cloud computing's principal advantage is its cost-effectiveness, as it removes the necessity to invest in and maintain in-house IT infrastructure. Using cloud computing services, a CRSP has the flexibility to scale up or scale down operations and storage as needed. Ability to scale also minimizes the risks involved in in-house operations and maintenance. Cloud computing also reduces the risk of downtime that could lead to a loss in productivity, reliability, and reputation. For example, having previous versions of credit reporting software stored in the cloud and running on multiple cloud availability zones allows faster recovery from disasters. If one zone goes down for any reason, the system will automatically failover to working regions without any interruption for users.

DLT permits secure sharing, viewing, and storing of digital information. Furthermore, its use of cryptography encryption brings security and transparency of data to new levels. Decentralized ledgers can secure the digital databases, making the system immune to cybercrime, as all copies stored across the network must be attacked simultaneously for any cyberattack to succeed. Decentralization also reduces operational costs and increases efficiency in the long run, providing more opportunities to work on separate projects simultaneously.

2.2.2. The Emergence of Alternative Credit Reporting Service Providers

New technologies combined with new data sources enable alternative credit reporting service providers to rapidly develop innovative products. The potential transformation of the financial industry by innovative entities has implications for the credit reporting systems as well. As strong innovators, globally active CRSPs closely follow developments in the fintech ecosystems. In the meantime, fintechs are emerging as competitors or challengers to the existing CRSPs and are filling gaps that the industry has not been able to address. Box 6 provides a non-exhaustive selection of case examples of companies involved in credit reporting activities.

Box 6: Case Examples of Alternative Credit Reporting Service Providers

Colendi, based in Turkey, uses a blockchain-based decentralized platform that leverages AI to generate credit scores based on alternative data. Its users authorize Colendi to read their data on smartphones or social media to be analyzed through integrated blockchain nodes.

Ledger Score, based in Estonia, offers users a credit scoring platform that leverages their cryptocurrency transactions data. It removes the anonymity of crypto transactions by digitally verifying individuals and businesses.

Future Finance, based in Ireland, produces credit scores for university students and offers affordable loans. Its proprietary algorithm predicts future loan affordability based on assessing continuation rates to school and employment rates after graduation.

Amartha in Indonesia developed AI/ML algorithms to evaluate the psychometric test results of women entrepreneurs in rural areas. They target a customer segment that often does not have access to mainstream financial services.

Nova Credit enables a consumer-driven, cross-border credit information sharing platform that allows individuals to transfer their credit reports from nine countries to the US to be transformed into a credit score applicable in the US.

Credit Vidya in India offers alternative data-based credit scores for first-time and underserved borrowers. It collects customers' digital footprints (e.g., contacts, SMS, location) and uses ML and big data analytics to assess creditworthiness.

Social Lender in Nigeria offers access to finance by assessing the social reputation of users on mobile, online, and social community platforms. Its algorithm performs a social audit of the user and calculates a social reputation score.

Farm Drive in Kenya focuses on alternative credit scores for smallholder farmers. It leverages mobile phones and other alternative data with ML tools and aims to close the credit information gap for farmers and help them access finance.

Cignifi in the US and Brazil leverages mobile phone data and other nontraditional data to help financial institutions and telcos serve underserved consumer segments. It uses proprietary big-data-based AI analytics tools.

Kiva, based in the US, uses a social underwriting process to evaluate creditworthiness. Kiva seeks financially excluded borrowers or businesses with positive social impact. In lieu of requiring credit scores, Kiva uses a social-network-driven fundraising tool to increase commitment to credit repayment.

2.2.3. Risks and Challenges

Innovations often come with operational and cyber risks. CRSPs are potential targets of cyberattacks, and data breaches can cause significant harm. Without effective information security and control environments and sound risk management, innovative technologies can expose CRSPs to cyber incidents. Also, data or model breaches can expose consumers to risk, as their personally identifiable data may be sold in black markets and make them targets for blackmails or scams. Breaches to models may also expose CRSPs to loss of trade secrets and competitive advantage as well as reputational risks. In addition, data breaches can ruin confidence in credit reporting systems and potentially affect the credit system as well.

Big data analytics is becoming a key source for CRSPs, bringing with it the responsibility to protect the confidentiality and security of personal and potentially sensitive data. Implementing big data systems bears the risk of infringing on consumer privacy and consent rights. Continuous availability of big data sources also raises concerns of over-dependency on third-party data providers.

Using alternative data sources heightens regulatory and compliance risks with respect to personal data protection legislation. Therefore, as is necessary under relevant regulations, CRSPs must undertake compliance assessments to ensure individuals are informed and have consented to have their data collected, processed, used, and shared.

Most big data sources are still not readily available, as most APIs and other information-sharing technologies are currently being developed. In addition, most entities still do not have procedures in place for sharing these data securely with the CRSPs. Big data is mainly being used to supplement the traditional data and still cannot serve as a stand-alone tool for assessing creditworthiness. Also, big data can be artificially manipulated, especially if nonfinancial data points are used as a stand-alone measurement.

Open third-party APIs inherently involve differences in security standards as the operations of the third-party provider (TPP) is not controlled by the CRSP. Thus, if the TPP does not comply with specific security measures, cyberthreats may affect the CRSPs. A reputational risk also arises from collaborating with TPPs. If the TPP engages in an unethical or other unfavorable practice, it would reflect negatively upon the CRSPs as well.

Open APIs create an ecosystem of collaboration in which customers are informed about all parties that can share their data. When operating through open APIs, the customer owns his/her data. However, if the security of the data is breached, CRSPs will not be able to use the information, as its validity will be questionable. CRSPs sharing APIs with third parties also risk being subject to phishing by cybercriminals who pretend to be fintech companies seeking to collect customer-related sensitive data.

Open banking ecosystems involve various stakeholders such as data providers, third-party providers, consumers, and government agencies. As such, if a dispute arises, the resolution mechanism becomes challenging and complicated. For example, a grievance filed by the customer could be due to an issue with any of the stakeholders. Due to the number of moving parts in the information-sharing ecosystem, however, linking the fault to a specific party will be difficult. A proper investigation and routing mechanism for dispute resolution is thus crucial.

Most AI/ML systems are considered black boxes that lack transparency as to how or why they reach a particular decision or score. However, consumers personally impacted by AI-based decisions can benefit from feedback on the reason for a rejection or a low score. This feedback is constructive, helping consumers build up their credit score or get loan approval in a following round. This challenges AI/ML systems, which may not be able to provide such feedback.

AI/ML systems may not uphold optimal decision-making and can produce unexpected outputs. In lending, ML models have the potential to replicate or amplify historical discrimination if faulty lending data was used to train the model. The biases could be due to the data used or to the humans that developed the systems. Bias risk becomes apparent when it is not possible to demonstrate how changes in individual data elements affect the output. Discrimination is suggested when an individual's credit score is lower, seemingly due to the AI's biased decision based on the individual's region, religion, political view, ethnicity, or sexual preference. Thus, while AI/ML removes the conscious and unconscious biases of human-based assessments, it also has the potential to impede progress in anti-discrimination practices in human judgments.

Unlike human assessors who can adapt to a given situation, AI/ML requires substantial amounts of historical data to predict future outcomes or develop a credit score. However, a primary requirement for both is a sufficient quantity of verified, accurate data. Without that, AI/ML will not derive a reliable prediction. The unavailability or inadequacy of such data to train/feed the AI/ML models is thus a significant challenge.

Biometric databases include vulnerable and sensitive personal information. Certain data can be locked with

passwords, while the biometric data itself cannot be changed. This carries the risk of false negatives when there are slight differences in the data subject, such as a change in facial complexion. The biometrics database can also be threatened by cybercriminals breaching the system and stealing data. As biometrics are used as secure authentication with less human checking, frauds may go unnoticed for extended periods. Digital ID systems also involve the risk of exploiting or controlling individuals through at-scale surveillance, social profiling, or algorithmic discrimination.

For several reasons, some digital ID systems are unable to cover most of the people for which they were intended to work. These include those unable to pay, but also individuals lacking correct documentation or who demonstrate digital illiteracy or resistance to digital ID technology. For example, the gov.uk service currently has a coverage success rate of 45 percent. Also, most jurisdictions lack proper functioning biometric regulations. As existing regulations are subject to change in each jurisdiction, and no globally accepted regulatory standard exists, lack of standardization affects the efficiency of biometric technologies. Also, it results in sub-par maintenance of the sensitive biometric data gathered.

Cloud computing raises potential risks that include the lack of visibility within cloud applications, theft of data from a cloud application, incomplete control over who can access sensitive data, and inability to monitor data in transit to and from cloud applications. Beside its benefits, cloud computing can result in third-party vendor risk. Cloud service providers and any outsourced third-party service providers must operate under robust standards and service levels. Due to the nature of its services, any interruptions in cloud computing systems directly affect the day-to-day operations of CRSPs. Any problems in the cloud services can also harm the resilience of the credit reporting system.

Cloud computing stores large amounts of sensitive and personal information for internal use. Unsecured internet connections can potentially increase the risk of cyberattacks. In the event of a security breach, cybercriminals could access information stored on credit reporting systems. In response to such risks, many data protection laws confine personal information, including credit and financial information, to within a country, constraining the credit reporting industry's use of cloud computing services.

DLTs provide decentralized, open, and permissionless services, but this is also a barrier to industry regulation, especially as no one owner can be identified as responsible. The uptake of DLT in the credit reporting industry has been for more private and permissioned ledgers such as digital ID systems. These use outsourcing regulatory frameworks, which bind the administrator/owner of the DLT providing services to the CRSP. However, going forward, it is likely that the technology will be regulated, and its effects on the already implemented technologies and their future remains uncertain.

While also being one of the main advantages, the main downside of DLT is that it creates an immutable database, which means information, once stored, cannot be deleted, and any updates are permanently recorded. Further, CRSPs face the risk of storing all personal data in one system. As the GDPR and many other data protection laws require personal data to be deleted after a specified period, using an immutable database conflicts with such requirements. Also, even though DLT has a great number of potential benefits, the technology is still in the experimental stage; its resilience in various environments has yet to be proven.

Certain consensus protocols used in DLT, such as "proof of work," use excessive amounts of energy, posing a novel environmental challenge. Unless greener ways of implementing DLTs (such as exploring methods of "proof of stake") are effectively employed, the benefits derived from the technology could be offset by its impacts on sustainability.

Chapter 3

Stocktake and Analysis of Responsible Use of Technology Frameworks

As use of disruptive technologies gradually increased, concerns arose over their possible unethical use or misuse. Therefore, international bodies and regulatory agencies have issued high-level principles, guidance documents, and regulatory directives on responsible technology use. This effort is still in its infancy, however, and only a few countries have implemented material guidance. In most cases, these directives have focused on the ethical use of AI/ML.

This section provides information on some of the key frameworks along with their scope and high-level principles, based on the main types of technologies, to shed light on the development of principles for responsible use of technology in the credit reporting industry. This selection relies on criteria such as the global applicability, relevance to the credit reporting industry, and suitability of the framework from the perspective of responsible technology use. Given the scale and broad scope of the issues, this selection is not exhaustive; for further reference, additional frameworks developed by policy makers, regulators, international organizations, and industry associations are briefly discussed in Appendix A.

3.1. Ethics and Human Rights for Responsible Use

Generally, frameworks on responsible use aim to address both ethics, and human rights. While ethics relates primarily to human values, human rights are primarily associated with human entitlements. The two are strongly linked, however, sharing two fundamental goals: protecting society from harm and enhancing citizens' quality of life (Gauthier 2009). To inform an organization's decision-making process, principles for responsible use of technology thus require an effective combination of approaches based on both ethics and human rights. A robust and holistic framework that can both realize benefits and mitigate risks will consider the two approaches as complementary. The rights-based approach is grounded in universally agreed international laws and norms, and the ethics-based approach covers broader issues such as fairness, inclusiveness, social justice, and cultural contexts. A rights-based approach provides a foundation for applying ethical principles, choices, and judgments (WEF 2020a).

Digital technologies provide new means to advocate, defend, and exercise human rights, but they can also be used to suppress, limit, and violate human rights (UN n.d.). Since existing human rights treaties were signed in a pre-digital era, possible protection gaps caused by evolving digital technologies remain to be addressed.

In response, the United Nations (UN) developed its Guiding Principles on Business and Human Rights (2011), calling on all business enterprises, regardless of size, sector, operational context, ownership, or structure, to respect human rights. The principles require businesses to do the following:

1. Avoid causing or contributing to adverse human rights impacts through their own activities, and address such impacts when they occur; and
2. Seek to prevent or mitigate adverse human rights impacts directly linked to their operations, products, or services or by their business relationships, even if they have not contributed to those impacts.

In particular, the UN advises that business enterprises should have in place policies and processes appropriate to their size and circumstances, including:

1. A policy commitment to meet their responsibility to respect human rights;
2. Human rights due diligence processes to identify, prevent, mitigate, and account for how they address their impacts on human rights; and
3. Processes to enable the remediation of any adverse human rights impacts they cause or contribute to.

The extensive use of digital technologies has also raised concerns from an ethics perspective. Mainly focusing on the use of AI, several countries and organizations have published ethical frameworks to address these concerns. For example, WEF issued the "Ethics by Design: An Organizational Approach to Responsible Use of Technology" (WEF 2020b). For ethical design, development, and deployment of technology, the paper suggests three design principles for incorporating and promoting ethical behavior into any organization's technology practices:

1. Attention: Timely reminders, checklists, frequent

refresher trainings, and other means to help ensure that ethical considerations are top-of-mind at crucial decision points.
2. Construal: Mission statements, deliberate choices of ethically freighted language, employee onboarding sessions, and periodic trainings involving ethical deliberation, and other interventions to promote ethical considerations.
3. Motivation: Encouraging prosocial actions, employing social "norm nudge" interventions, and other culture-change activities to motivate ethical behavior.

3.2. Big Data

The United Nations Development Group (UNDG) issued a guidance note on big data, focusing on data privacy, ethics, and protection and applicable to all member entities within the UN (2017). The guidance note is designed to establish common principles across UNDG to support the operational use of big data to achieve sustainable development goals; serve as a risk-management tool, taking into account fundamental human rights; and set principles for obtaining, retaining, using, and assuring quality control for private sector data. The principles covered include the following:

1. Data should be obtained, collected, analyzed, or otherwise used through lawful, legitimate, and fair means.
2. Any data use must be compatible or otherwise relevant and not excessive in relation to the purposes for which it was obtained.
3. A risks, harms, and benefits assessment that accounts for data protection and data privacy, as well as ethics of data use, should be conducted.
4. Stricter standards of data protection should be employed while obtaining, accessing, collecting, analyzing, or otherwise using any type of sensitive data.
5. Robust technical and organizational safeguards should be implemented to ensure proper data security management throughout the data lifecycle.
6. Data access, analysis, or other use should be kept to the minimum amount necessary to fulfill its purpose, and the amount and granularity of data should also be limited to the minimum necessary.
7. Data should be validated for accuracy, relevancy, sufficiency, integrity, completeness, usability, validity, and coherence and should be kept up to date.
8. Appropriate governance and accountability mechanisms should be established to monitor compliance with relevant laws and the highest standards of confidentiality and moral and ethical conduct with regard to data use.
9. Third-party collaborators engaged in data use should act in compliance with relevant laws, as well as the highest standards of confidentiality and moral and ethical conduct.

Similarly, International Committee on Credit Reporting (ICCR) issued a guidance note on the Use of Alternative Data to Enhance Credit Reporting. The report outlines several policy recommendations to promote the adoption and use of alternative data for credit reporting, while mitigating the risks inherent in such use (ICCR 2018). The recommendations particularly relevant to the use of technology include the following:

1. Increasing the availability of unique identifiers for individuals and businesses.
2. Providing access to national ID databases for validation purposes.
3. Promoting the development and provision of access to open data systems and standards.
4. Increasing the availability of digital footprints by promoting the use of digital platforms and digitization of the services of relevant government agencies.
5. Assessing the feasibility of implementing global unique identifiers for businesses or individuals for cross-border use and data sharing.

3.3. Open Banking & Open APIs

Open banking ecosystems vary across jurisdictions. In jurisdictions with no specific regulatory intervention, such as the US or Singapore, bilateral agreements between banks and third parties can set the conditions for access to banks' APIs, security and data protection requirements, and other obligations for each party. In other jurisdictions, such as Japan or Hong Kong, high-level regulatory guidelines for open banking rely on banks for specifics. In jurisdictions with mandatory open banking models, banks are required to grant third-party access to bank accounts, accompanied by a regulatory framework that sets a specific regime for the third parties (EU).

As an example, the Open Banking Implementation Entity (OBIE) in the UK developed standards and guidelines to foster the use of open banking. The standards include the principles for informed decision-making, simple and easy navigation, parity of experience, and familiarity and trust, all intended to enable a well-designed data sharing experience while protecting vulnerable customers. The principles outline the following:

1. Transparency of choice, action, and the consequences of actions for clarifying rights and responsibilities of data sharing and how the relationship works.
2. Control, maximizing the customer's sense of control over what data is shared and its data frames, enabling users to make informed decisions and choices.
3. Speed appropriate to the customer and the data sharing experience undertaken.
4. Security precautions, with explicit clarity and reassurance

in relation to data definition, use, and protection.

The principles of control, speed, transparency, and security overall aim to create a trust environment for the customer (OBIE n.d.).

3.4. AI/ML

AI/ML use to assess creditworthiness is under the radar of regulatory authorities regarding data privacy, transparency in models, and fairness and explainability of outputs. Most regulations protect to some degree against discriminatory practices in credit scoring (e.g., in the US and the EU). The use of AI/ML is an area of particular concern, however, as some of these propriety algorithms work as black boxes, rendering their decision-making methods only inconsistently transparent. In the US, AI models must address the adverse action notice requirements of the Fair Credit Reporting Act (FCRA), which applies when denial of a loan application is based in whole or in part on a credit score obtained from a CRSP; creditors must disclose the key factors that adversely affected the score. The EU has proposed a regulation to introduce harmonized rules on AI, following a risk-based approach to protect the fundamental rights and safety of individuals and businesses, while supporting innovation (EU 2021). In line with a risk-based approach, AI systems falling into the high-risk category include credit scoring models. In this sense, credit scoring models that use AI will be subject to strict obligations such as:

1. Adequate risk assessment and mitigation systems and appropriate human oversight to minimize risk.
2. High-quality datasets feeding the system to minimize risks and discriminatory outcomes.
3. Logging of activity to ensure traceability of results.
4. Detailed documentation with all necessary information for authorities to assess compliance.
5. Clear and adequate information to the data subjects.
6. High level of robustness, security, and accuracy.

The ethics perspective of AI/ML requires policy considerations on a broader level. Many policy frameworks for AI/ML use have been published globally. For example, the Monetary Authority of Singapore (MAS) published principles to promote fairness, ethics, accountability, and transparency (FEAT) in the use of AI and data analytics for the financial sector (MAS 2018). The principles provide high-level guidance on justifiability, accuracy, and bias, ethics, internal and external accountability, and transparency. ICCR, too, recommends that credit scoring models be explainable, transparent, and fair. The data used and the decisions made on the basis of credit scoring should operate within equal opportunity or anti-discrimination laws (ICCR 2019a). An overview of common regulatory principles relating to AI/ML use in comparison with traditional credit scoring models appears in Table 1.

UNESCO recently published the first global standard-setting instrument on the ethics of AI in the form of a recommendation (UNESCO 2021) providing the following principles:

1. Proportionality and do no harm
2. Safety and security
3. Fairness and non-discrimination
4. Sustainability
5. Right to privacy and data protection
6. Human oversight and determination
7. Transparency and explainability
8. Responsibility and accountability
9. Awareness and literacy
10. Multi-stakeholder and adaptive governance and collaboration

Principle	Common Themes
Reliability/ Soundness	In general, expectations are similar as those for traditional models. For AI models, assessing reliability and soundness of model outcomes is viewed from the perspective of avoiding harm (e.g., discrimination) to consumers.
Accountability	Similar to expectations outlined in general accountability or governance requirements, but human involvement is viewed as more necessary. For AI models, accountability includes "external accountability" to ascertain that data subjects (e.g., prospective or existing customers) are aware of AI-driven decisions and have channels for recourse.
Transparency	Similar expectations as related to explainability and auditability. For AI models, external disclosure (e.g., data used to make AI-driven decisions and how the data affects the decision) to data subjects is also expected.
Fairness	Stronger emphasis in AI models. Expectations on fairness relate to addressing or preventing biases in AI models that could lead to discriminatory outcomes, but otherwise "fairness" is not typically defined.
Ethics	Stronger emphasis in AI models. Ethics expectations are broader than "fairness" and relate to ascertaining that customers will not be exploited or harmed, through bias, discrimination, or other causes (e.g., AI that uses illegally obtained information).

Table 1: Common AI/ML Principles (Yong 2021)

3.5. Digital ID & Biometrics

Digital identification tools are key to increasing the coverage of credit reporting systems. The World Bank issued principles on identification for sustainable development in the digital age. The document, as endorsed by the UN and several national and international organizations and international financial institutions, outlines the following key considerations:

1. Ensuring universal access for individuals, free from discrimination.
2. Removing barriers to access and use.
3. Establishing a trusted (unique, secure, and accurate) identity.
4. Creating a responsive and interoperable platform.
5. Using open standards and preventing vendor and technology lock-in.
6. Protecting privacy and agency through system design.
7. Planning for financial and operational sustainability.
8. Protecting personal data, maintaining cyber security, and safeguarding people's rights through a comprehensive legal and regulatory framework.
9. Establishing clear institutional mandates and accountability.
10. Enforcing legal and trust frameworks through independent oversight and adjudication of grievances.

CRSPs use biometrics in a range of products. The Biometrics Institute identifies the following seven principles for addressing ethical issues relating specifically to biometrics.

1. Ethical behavior, that is, avoiding actions that harm people and the environment beyond legal requirements.
2. Ownership of the biometric and respect for individuals' personal data, as treated with the utmost care.
3. Serving humans, which entails accounting for public good, community safety, and net benefits to individuals.
4. Justice and accountability, by accepting principles of openness, independent oversight, accountability, and the right of appeal and appropriate redress.
5. Promoting privacy-enhancing technology of the highest quality for accuracy, error detection, and repair, with robust systems and quality control.
6. Recognizing the dignity of individuals and families, in line with the UN Universal Declaration of Human Rights.
7. Equality, entailing preventing discrimination or systemic bias.

3.6. Cloud Computing

The International Organization of Securities Commissions (IOSCO) developed its guidance document on the Principles on Outsourcing, updating it to cover cloud service providers (CSP). The document outlines the following principles for credit reporting activities by cloud services:

1. Conduct suitable due diligence in selecting an appropriate CSP and monitoring its ongoing performance.
2. Enter into a legally binding written contract with each CSP, the nature and detail of which are appropriate to the materiality or criticality of the outsourced task.
3. Ensure both the CRSP and any CSP establish procedures and controls to protect proprietary and client-related information and software and ensure a continuity of services, including a plan for disaster recovery, with periodic testing of backup facilities.
4. Ensure that CSPs protect confidential information and data related to the regulated entity and its clients, from intentional or inadvertent unauthorized disclosure to third parties.
5. Be aware of the risks posed and manage them effectively, where the CRSP depends on a single CSP for material or critical outsourced tasks or where it is aware that one CSP provides material or critical outsourcing services to multiple entities including itself.
6. Ensure that the CRSP's regulator, its auditors, and itself are able to obtain promptly, upon request, information concerning outsourced tasks relevant to contractual compliance and/or regulatory oversight, including, as necessary, access to the data, IT systems, premises, and personnel of CSPs relating to the outsourced tasks.
7. Include written provisions relating to the termination of outsourced tasks in the CRSP's contract with CSPs and ensure that the CRSP maintains appropriate exit strategies.

3.7. Distributed Ledger Technologies

The International Telecommunication Union (ITU), as the UN's specialized agency for information and communication technologies, published a technical paper that discusses the key features of DLT and its associated regulatory challenges (ITU 2019b). Examples of approaches that users, regulators, and solution providers could use to address these challenges are discussed in the paper, along with the following recommendations:

1. Distribution and ledger sharing: Civil and criminal liability for blockchain distributed control, decentralized controllers/managers (human or not), authoritative sources of records and data, and DLT-record and other related digital sources of legal proof.
2. Autonomy and responsibility: Considering pro-transparency measures early at the design stage, setting on-chain dispute resolution tools on a case-by-case basis prior to an off-chain solution, to be complemented by consumer protection regimes, and increasing the level of trust with tools like certification of smart contracts.

3. Tamper evidence and resistance: Framework standardization for use of symmetric cryptography, enhanced public key infrastructure standardization, avoiding storing clear-text personal data on blockchain, using sidechains or other private storage options for sensitive data, using zero-knowledge proofs where possible, applying additional measures when storing hashes of personal data, avoiding relying solely on consent in the context of personal data, and performing a data protection impact analysis.
4. Incentive mechanism and digital assets: Consider developing interoperability specifications at the right levels where appropriate.
5. Openness, transparency, and anonymity: Adjust the level of openness and transparency of the DLT protocol in accordance with relevant regulations.

Chapter 4

Principles for the Responsible Use of Technology in Credit Reporting

The principles discussed here are meant to ensure responsible technology use in credit reporting activities. Applying the proposed principles will help the credit reporting industry make the best, most responsible use of disruptive technologies to the benefit of all stakeholders. To ensure this objective, the principles are written to apply to all types of technologies used in credit reporting activities rather than to specific technologies or types of CRSPs. This is particularly important given the evolving nature of credit reporting systems as technology advances.

This section outlines ten principles for responsible use of technology in credit reporting (Box 7). Participants in credit reporting systems are expected to apply the principles according to their use of the technologies. The principles are not mutually exclusive from one technology to another, and should be considered in their totality. Finally, as noted, the principles are technology agnostic: they do not focus on specific systems, software, or technology and should be applied regardless of development language or data storage methods.

1. **Fairness**
Credit reporting systems should ensure the fair use of technologies deployed in their operations. Technology-driven credit reporting products should at all times protect the fundamental rights of individuals and should not discriminate against any individuals, groups of consumers, or SMEs.

2. **Ethics**
Credit reporting system participants should ensure that any technology they adopt and use complies with their corporate values, codes of conduct, and highest ethical standards. Technology-driven decisions should be held to at least the same ethical standards as human-driven decisions.

3. **Accountability**
Credit reporting system participants are accountable for the use of both internally developed and externally resourced technologies. Appropriate governance mechanisms should be in place to oversee the processes of technology-driven credit reporting products.

4. **Transparency**
Credit reporting system participants should ensure that the techniques and methods used in their technology-driven decisions are explainable, assessable, and understandable by relevant stakeholders.

5. **Security and Robustness**
Credit reporting systems should be governed by an appropriate data security framework to ensure the confidentiality, integrity, and availability of information at all times. The robustness of technologies should be ensured to avoid unintentional harm to individuals.

6. **Lawfulness**
Credit reporting system participants should ensure that the use of data and technologies is lawful and complies with relevant regulations and professional standards.

7. **Privacy**
Credit reporting system participants should protect the privacy of data subjects while accessing, collecting, analyzing, processing, and distributing their data for credit reporting.

8. **Sustainability and Well-Being**
Technologies employed in credit reporting systems should support human well-being and be sustainable in all human, social, cultural, economic, and environmental aspects.

9. **Inclusivity**
The adoption and use of technological innovations in credit reporting systems must not result in or accentuate the exclusion of any individual or group of individuals.

10. **Trust**
Technologies employed in credit reporting systems should be considered trustworthy in the eyes of stakeholders, including data subjects and financial institutions.

Box 7: Principles for Responsible Use of Technology in Credit Reporting

4.1. Principle 1: Fairness

Credit reporting systems should ensure the fair use of technologies deployed in their operations. Technology-driven credit reporting products should at all times protect the fundamental rights of individuals and should not discriminate against any individuals, groups of consumers, or SMEs.

CRSPs should ensure both the substantive and the procedural fairness of their products. Substantive fairness ensures that individuals and groups are free from unfair bias, discrimination, and stigmatization and that in creating equal opportunity in terms of access to financial services due care is taken to ensure technology use does not lead to individuals being unjustifiably impaired. Over and above these points, procedural fairness assures individuals they have the ability to contest and seek effective redress against technology-driven decisions and CRSPs.

CRSPs should ensure that use of AI/ML does not result in bias and discrimination against individuals or protected groups; rather, it should promote positive discrimination of previously marginalized people. Beyond potential algorithmic bias, CRSPs should ensure that the underlying training data on which AI/ML systems are built are inclusive and unbiased by implementing pre-processing techniques like optimized pre-processing, suppression, massaging, reweighing, and sampling. In addition, in-processing techniques such as adversarial debiasing, regularization, or surrogate models, and post-processing techniques, like statistical calibration, should be employed to ensure models are fair. CRSPs should categorically consider human rights at every stage of AI/ML systems development and endeavor to conduct a search for the least discriminatory alternative models prior to deployment.

CRSPs should establish a model governance framework and an AI/ML-specific risk management framework for credit scoring models to ensure scores are fair. Scoring models should use lawfully obtained, clear, understandable, disclosable data. Rigorous validation, testing, and back-testing of models should be performed to confirm the accuracy and reliability of technology-driven outputs. In addition, the methods and techniques employed should be independently assessable and auditable.

CRSPs should ensure the fairness of biometric systems used in their services. Sensitive information such as gender or race identifiable through biometrics should only be employed to verify identity and should not be accessible for any other subjective assessment tools.

4.2. Principle 2: Ethics

Credit reporting system participants should ensure that any technology they adopt and use complies with their corporate values, codes of conduct, and highest ethical standards. Technology-driven decisions should be held to at least the same ethical standards as human-driven decisions.

CRSPs should establish and maintain the highest level of ethical standards in the use of technology. Appropriate tools such as mission statements, periodic trainings, and social activities should promote ethical behavior throughout the organization. The ethical standards of a CRSP should also be supported by codes of conduct and human-centered corporate values. Ethical considerations should ensure that individuals are not in any way exploited or harmed through bias, discrimination, or any other means, such as unlawfully obtained information.

CRSPs should recognize the dignity and equal rights of individuals and should use technology and in a way that serves humans, taking into account the public good, community safety, and net benefits to individuals.

AI/ML-based systems should operate in line with the highest ethical standards for CRSPs. The ethical considerations in the use of AI/ML should be monitored by appropriate human agency and oversight. CRSPs should ensure staff dealing with AI/ML systems are adequately trained to interpret AI model output and decisions and to detect and manage data bias. To contribute to objectivity and respect for various perspectives, needs, and objectives, staff teams that design, develop, test, and deploy AI/ML systems should reflect the diversity of users and of society in general.

4.3. Principle 3: Accountability

Credit reporting system participants are accountable for the use of both internally developed and externally resourced technologies. Appropriate governance mechanisms should be in place to oversee the processes of technology-driven credit reporting products.

AI/ML-based systems used at CRSPs should be governed by an appropriate internal accountability mechanism. Decision-making processes driven by AI/ML should be tested, monitored, approved, and authorized by responsible authorities throughout the organization. The board of directors and senior management are accountable for the use of AI/ML systems, including self-learning algorithms. Senior management should develop, with board approval, a clearly defined model governance framework to establish the roles and responsibilities in developing and monitoring AI/ML system operations.

The explainability, traceability, and auditability properties of AI/ML systems should allow independent third parties to assess and develop qualified opinions. The decision-making process in these systems should be appropriately traceable for human oversight in testing, validation, back-testing, and calibration phases.

An appropriate validation process should be in place for AI/ML-based systems prior to their use for credit reporting. This initial validation should be performed or at least examined by an independent function not involved in the original modeling process. For ongoing validation at regular intervals, factors that trigger ad hoc validation and recalibration of the AI/ML system should be determined.

CRSPs are accountable for the extraction of alternative data and the design of AI/ML algorithms and processes and should provide accessible redress mechanisms. Data subjects should have available appropriate communication channels to enquire about, appeals, and request review of AI/ML-based decisions that affect them. Verified and relevant supplementary data provided by data subjects should be taken into account when performing such reviews.

CRSPs are accountable for the services provided to the consumer and for the proper use of data accessed through APIs. Data providers and CRSPs are both accountable for ensuring data security when using APIs. Accountability in terms of API technology lies with the ultimate aggregator/collector of the API data, which should be accountable to customers in any dispute. A responsible data management model covering legal and other concerns should be established with clearly defined ownership and liabilities for all parties.

CRSPs are accountable for managing the biometrics and digital identification data and their security to the extent they act as collecting agencies of such data. The roles and responsibilities should be defined for designing and managing the privacy protection of biometrics data.

CRSPs are accountable for assessing, managing, and monitoring their relationship with cloud service providers as well as other third-party vendors. Outsourcing policies and processes should cover the conduct of appropriate due diligence for selecting service providers, managing the risks associated with outsourcing agreements, maintaining an effective control environment over data, and establishing viable contingency plans to ensure business continuity.

4.4. Principle 4: Transparency

Credit reporting system participants should ensure that the techniques and methods used in their technology-driven decisions are explainable, assessable, and understandable by relevant stakeholders.

CRSPs should disclose to the public its credit reporting activities, technology policies, ethical values, and codes of conduct. CRSPs should proactively disclose the use of AI/ML-based systems, their implications, and the measures to mitigate potential risks to data subjects and other stakeholders. Use of AI/ML based systems should be transparent in terms of their use, the extent of data feeding the systems, and how the system produces its particular outcomes.

AI/ML systems should be explainable and interpretable by relevant stakeholders. CRSPs should be able to provide data subjects, upon request, clear explanations on the data used to make AI/ML-driven decisions about the subject and how the data affects the decision. Disclosures to data subjects should be in the form of plain information on the factors forming the basis for the decision. The elements should each be shown separately to identify the relative weight or significance they bear on the final decision, along with the detailed logic on why that driver would be calculated as a positive or a negative factor within the model.

Adequate documentation should be provided that AI/ML-based systems can be verified by independent third parties. In particular, the selection process of the model, model calibration and training, and model validation procedures must be adequately documented. AI/ML-based models should be traceable in the sense that their decisions, and the datasets and processes that yield the decisions, are documented in an easily understandable way.

CRSPs using big data and/or alternative data should be transparent on the types and sources of data and the process for gathering, storing, and using it. The types of data that provide the basis of credit reporting products should be clear, understandable, and disclosable to the data subjects.

CRSPs should be transparent about their dealings with data subjects' biometric data. Biometric data should only be shared with third parties if required, and only after obtaining the individual's unambiguous and informed consent. Data subjects should be able to know at any given time the extent of information accessed about them, and CRSPs should provide simple, fast, and efficient procedures that allow data subjects to withdraw consent at any time and without any undue delay or cost or any gain to the collector/holder of such information.

CRSPs should be transparent in their use of cloud service providers, particularly in data management. CRSPs should ensure that information concerning outsourced tasks relevant to data subjects, data users, and data providers is disclosed appropriately to the relevant stakeholders.

4.5. Principle 5: Security and Robustness

Credit reporting systems should be governed by an appropriate data security framework to ensure the confidentiality, integrity, and availability of information at all times. The robustness of technologies should be ensured to avoid unintentional harm to individuals.

CRSPs should develop and employ an appropriate data security framework, reviewed and updated as needed, that accounts for potential risks associated with the use of new technologies. The framework should cover effective board oversight, clearly defined and documented roles and responsibilities for information security functions, and allocation of adequate staff with necessary qualifications and appropriate budgets to ensure sound management of information security and cyber risks. CRSPs should employ control and risk mitigation tools for data management, such as minimum access, access recertification, user accountability, activity logs, or authentication measures. Regular cyber audits should assess and assure the safety and soundness of credit reporting activities against cyber risks, with a risk-based approach.

AI/ML systems should be verifiably safe and secure throughout their processes. AI/ML should be developed and used in a technically robust way to ensure that they reliably behave as intended while unintentional and unexpected harm is minimized and unacceptable harm is prevented. AI/ML systems should be protected against confidentiality and integrity attacks on their architecture and underlying data to avoid adversarial outputs to data subjects or CRSPs. CRSPs should ensure AI/ML systems are robust against potential vulnerabilities such as data poisoning, adversarial attacks, or model extraction attacks that could lead to unreliable outputs. Sufficiently robust models can contribute toward building trust in AI/ML system output.

Outsourcing policies for third-party providers should include appropriate and proportionate consideration of minimum cybersecurity standards, data retention periods, data encryption requirements, network security processes, and cyber incident handling plans.

4.6. Principle 6: Lawfulness

Credit reporting system participants should ensure that the use of data and technologies is lawful and complies with relevant regulations and professional standards.

CRSPs should ensure that data is accessed, collected, analyzed, processed, and used through lawful and legitimate means. Appropriate governance mechanisms should be established to monitor compliance with relevant laws and the highest standards of ethical conduct with regard to data use. Third-party providers engaging with data should also act in compliance with applicable laws and the highest standards of confidentiality and moral and ethical conduct.

CRSPs should have in place an effective compliance function with an adequate number of staff with the necessary qualifications and experience to manage the legal and compliance risks of technology use. Any engagement with new technologies, dealings with third-party technology providers, or accessing new sources of data should be subject to a robust evaluation process to ensure lawfulness. CRSPs should also ensure that the technologies employed comply with the technical and professional standards issued by relevant standard-setting organizations.

4.7. Principle 7: Privacy

Credit reporting system participants should protect the privacy of data subjects while accessing, collecting, analyzing, processing, and distributing their data for credit reporting.

CRSPs should have in place an effective data governance framework, including a risks, harms, and benefits assessment that accounts for data protection and data privacy. The framework should recognize the dignity of individuals and include concrete protections for human rights as well as the ethics of data use.

Access, processing, analysis, or other use of personal data should be kept to the minimum amount and granularity needed to perform credit reporting activities. Stricter data protection standards should be used when dealing with any type of sensitive data. Robust technical and organizational safeguards should be implemented to ensure proper data security management.

CRSPs employing DLT in their activities should develop appropriate policies to protect the privacy of personal data and ensure compliance with relevant legal requirements to delete personal data, while respecting the transparent and immutable structure of DLT systems.

4.8. Principle 8: Sustainability and Well-Being

Technologies employed in credit reporting systems should support human well-being and be sustainable in all human, social, cultural, economic, and environmental aspects.

CRSPs should prioritize human well-being as an outcome in the development, design, and deployment of technology by using the best available, most widely accepted metrics for well-being as a reference. In assessing the physical and mental impacts of technology use on individuals, CRSPs should also consider technology policies from a broad social

perspective.

CRSPs should assess the overall process of technology development and use in terms of sustainability and impacts on the environment. Use of resources and energy consumption should be considered in terms of efficiency, effectiveness, and minimizing harm.

Use of DLT in CRSPs should be optimized to use fewer energy resources and minimize climate effects. Greener ways of using DLTs should be explored to limit environmental impacts.

4.9. Principle 9: Inclusivity

The adoption and use of technological innovations in credit reporting systems must not result in or accentuate the exclusion of any individual or group of individuals.

Adoption of any technological innovations by CRSPs should not exclude or disadvantage any communities or individuals. CRSPs should employ technologies that are inclusive by design to assure that the design processes lead to products usable by all groups of people, particularly those traditionally excluded. These technologies should provide open and fair services to all groups of consumers, regardless of any personal characteristics or protected attributes.

Particular attention during model design and AI/ML system use should ensure that models incorporate underserved segments of the economy at risk of exclusion from modelling data sets.

Digital identification systems should serve all customers without excluding any personal attributes such as any physical traits or literacy levels. Particular care should be taken to ensure that information collected for verification is acceptable in terms of protecting human rights.

4.10. Principle 10: Trust

Technologies employed in credit reporting systems should be considered trustworthy in the eyes of stakeholders, including data subjects and financial institutions.

New technologies introduced by CRSPs should not adversely impact the reliability and trustworthiness of credit reporting systems. CRSPs should ensure that the technologies they introduce will increase efficiency and not undermine service quality. Due to the credit reporting industry's key role in the financial sector of any economy, before new technologies are implemented, due care must be taken to anticipate how they will be perceived by the ultimate users.


AUDIO
CREDIT/ATM CARD
CHANGE & RECEIPT

Chapter 5

Considerations for Implementing the Principles

5.1. Applying the Principles

Like any other ethics-based or rights-based framework, the principles are not a set of fixed rules to adapt and comply with. Nor are they technical standards that a CRSP can simply apply as one-off action items. Rather, the principles require an organization-wide adaptation with ongoing efforts to understand the impacts and implications of technologies, maximize the technologies' benefits while eliminating or minimizing their harms, distribute benefits and burdens, and develop diverse perspectives for navigating dilemmas and solving conflicts. Applying the principles requires commitment from CRSP leadership and the organization as a whole.

Assessing responsibility for observing the principles primarily lies with a CRSP's board of directors. Assessing current practices against the principles should identify weaknesses and assist in defining areas for improvement. CRSPs can communicate the results of this compliance assessment to the public. Assessments can be done by either the ethics board or similar body or by external assessors, as appropriate. Assessors should gather the facts necessary to develop conclusions regarding each principle. To gain a general understanding of and analyze the existing situation relating to the principles and key considerations associated with them, assessors can use questions such as the illustrative ones listed below.

Model Design

1. Is the AI/ML model applicable and appropriate for its intended purpose?
2. Is the AI/ML model ethical?
3. Do AI/ML developers have training in ethics, human rights, and civil rights? How diverse is the team that develops AI/ML products and services?
4. How is the sustainability impact of technologies assessed?
5. Does an ethics board or similar committee assess the potential risks and mitigate them throughout the development and deployment of the model?

Data Use

1. Is the data lawful and legitimate? Should the data be used?
2. What are the precautions for identifying and eliminating types of data that can act as proxies for protected attributes?
3. How is the lawfulness of data collection ensured with regard to sources of nontraditional data?

Data Governance

1. What is the quality of the data?
2. Is the data accurate and fit for purpose?
3. How are the risks of inaccuracy and bias assessed and managed?

Model Documentation

1. Is there appropriate documentation in place for using the AI/ML systems?
2. Is there a proper traceability process in place throughout the documentation?
3. Does documentation include logging activities of staff with access to sensitive data?
4. Are roles and responsibilities clearly identified for deploying the model ethically?

Outcome Analysis and Controls

1. Is there an effective control framework in place?
2. Is there an effective human oversight mechanism in place?
3. Is a grievance mechanism in place for individuals impacted by the outputs of technology-driven decisions?
4. Is there a process for providing accurate information to data subjects regarding the use of AI/ML?

Tuning and Monitoring

1. How often are results validated?
2. Is there an ongoing monitoring process in place?
3. Is there an established mechanism to identify and correct unintended results following from the decisions of AI/ML systems?
4. Which measures are in place to protect individuals' privacy?

5.2. Capacity Building

Many of the disruptive technologies in the credit reporting industry are relatively new, and limited information or knowledge surrounds them. Using these technologies to their optimum potential requires understanding the technologies in the context of all relevant stakeholders and the trainings provided to key staff working with them. Improving policy makers' and CRSPs' technical proficiency is of foremost importance for successfully implementing every one of these technologies. Capacity building for a thorough understanding of the credit reporting industry's technology infrastructure is key for rolling out new technologies efficiently and responsibly. Capacity-building activities should also cover understanding and implementing the principles for responsible technology use. While the responsibility for facilitating training primarily lies within the CRSP, regulatory authorities can promote training in their respective jurisdictions.

Industry associations of CRSPs can also play an important role in capacity building for responsible technology use. The credit reporting industry has a long history of being largely self-regulated. Considering the technical details and associated risks in credit reporting systems, the industry developed its own Codes of Conduct. In this sense, self-regulatory mechanisms developed within credit reporting industry associations in many jurisdictions and at the regional level. Considering the highly technical nature of credit reporting activities, these associations can promote the implementation of the principles in various ways, such as by creating guidance documents on assessment methodology of the principles, developing open-source toolkits for responsible innovation, and facilitating trainings on areas of key concern.

5.3. Technology-Specific Recommendations

AI/ML algorithms use supervised and unsupervised learning techniques to analyze the data sets fed into them. These systems are built to perfect over time their models, the data they gather, and the results and correlations of historical predictions. If the amount of data available is limited or low quality, however, AI/ML models can require human intervention to rectify any undesired decisions. Interventions such as human-in-the-loop or human-on-the-loop should be used as appropriate to review the model's results and correct any undesired biases until the algorithm properly "learns" to produce reliable results in the long run. Therefore, the AI/ML system's degree of autonomy should be clearly defined, and the different levels of human control over the system should be clearly identified based on the specificities of each use case. An appropriate combination of human oversight and AI should safeguard the system, establishing a continuous loop of training, testing, fine-tuning, validating, and monitoring the AI/ML algorithms.

Big data analytics systems should be managed with a big data governance and risk management framework to ensure appropriate policies and procedures are maintained for different data sets and objectives. Policies on collecting and keeping the minimal amount of data will limit risks related to privacy issues and mitigate potential discriminatory practices based on collection of nonessential and nonbearing information. Minimality also helps produce comprehensible, reliable outputs, as only relevant information is fed into the system, essentially reducing both the variety and the volume of data.

Open APIs provide access to a larger amount of information than required, hence it is important to determine the responsibilities of each collaborator or TPP for managing privacy concerns and security breach risks. A clearly defined responsibility matrix enables every party involved in the open API ecosystem to focus on their respective scope and work. In addition, appropriate dispute resolution mechanisms should be in place for handling customer complaints and infrastructure failures involving data providers and TPPs.

Biometric systems must be secure and robust enough to handle bad actors, fraud, and abuse without creating additional burdens for end users. The checks and procedures in place should be located between extreme innovation and conservative security, as the security of the system cannot be compromised in the interests of innovation and user-friendliness. Digital ID systems should be designed and built using a human-centric approach that recognizes the diversity of cultures and inherent human qualifications. A well-established human-centric approach will help eliminate or minimize potential exclusions by these technologies. In addition, adaptive technologies, such as multimodal biometrics, can be leveraged so that the system can use multiple biometric traits to adjust to new behavioral characteristics.

Third-party cloud service providers should adhere to the same principles as does the credit reporting industry, including the relevant principles laid out in the previous section, such as ethics, accountability, security and robustness, privacy, lawfulness, and sustainability. Compliance by cloud service providers with key regulatory rules such as data access, control, storage, or removal of sensitive data should be of concern to the CRSPs.

While DLT has specific advantages due to its inherent qualities, such as immutability and transparency, special attention is needed to its extreme use of computing power and resources. Thus, relevant pieces of evidence should be shared and verified for the specific use cases to ensure DLT

use makes sense. Further, it might be suitable to run the requirement through a blockchain ethical design framework to ensure that the distributed infrastructure is the most viable option for the solution being developed.

5.4. Use Cases

Credit reporting system participants can benefit from considering the following use cases as illustrative examples of applying the principles. The use cases demonstrate how different types of CRSPs — big or small, local or international — can implement or align their governance practices with the principles.

Use Case 1: Fairness & Inclusivity

The CRSP conducts regular reviews to ensure its AI/ML-based credit scores are fair. The team responsible for developing the credit scoring model maintains a data mapping exercise that allows tracing all data used to their respective sources. The map helps identify the data source even after transformation and aggregation. The model uses different datasets for training, testing, and validation. The datasets used do not include protected class attributes, and variables that could serve as proxies for protected class attributes are removed. The dataset has been assured to be inclusive in the sense that it does not categorically exclude any groups of customers with protected attributes. Further, a disparate impact that can occur even absent using protected class or proxy variables is evaluated and tested at each stage of the model development cycle.

The staff team tracks model outputs regularly to ensure the reliability, accuracy, and consistency of the AI/ML model. The results from the training, back-testing, and validation stages are used as a benchmark for the model outputs for fine-tuning at the post-deployment stage. Fairness reviews occur at the appropriate minimum intervals to ensure that the models do not cause disparities due to changes in the dataset. For example, the model is tested for bias (e.g., representation bias, measurement bias) regarding borrowers' sex (male as a privileged group; female as an unprivileged group) against default thresholds. If the results of the test reveal a bias against the unprivileged group, appropriate techniques are applied to mitigate the bias, such as data weighting or resampling in pre-processing, adversarial debiasing in-processing, or label modification post-processing.

Use Case 2: Ethics

The CRSP created an ethics board that guides the organization through the ethical development and deployment of technologies. While the ethics board draws up the principles for the company's technology ethics, it also has appropriate powers and resources necessary to put the principles into practice. Relevant business units and functions are represented on the ethics board, sharing responsibility for providing governance on ethical issues pertaining to technology use for the overall organization. The CRSP encourages its staff to provide feedback when a technology's output appears biased or suboptimal. The ethics board empowers technology users to share their experiences to enhance trust in the AI/ML systems. Finally, employees are appropriately involved in interpreting and using AI/ML-based outputs when making decisions.

Use Case 3: Accountability

Senior management at the CRSP established strategies, guidelines, and rules for use of AI-based decision-making processes. Employees receive adequate training to raise awareness of the principles for responsible use of technology. Trainings also cover legal frameworks applicable to AI/ML system use. Appropriate mechanisms are in place to allow redress of any harm or adverse impact to data subjects. Relevant third parties or employees can also report potential vulnerabilities, risks, or biases in the AI/ML systems.

The CRSP established both internal and external audit mechanisms to ensure the accountability of its AI/ML systems. Assessments are made in model design and performance, implementation, governance, and documentation. The internal audit team reviews the documentation, including the system's intended function and performance, the model architecture, datasets used in training and testing, checkpoints for reviewing and validating datasets, and organizational processes to monitor system operations. Focused audits are performed regularly in which a specific dataset feeds the system to allow review of the outputs to check for bias in the system or unexpected results. These focused audits also serve to stress test the processes that produce credit reports or other products. Where appropriate, code reviews are conducted by internal or external audit resources, provided that the privacy of any personal data is preserved.

Use Case 4: Transparency

The CRSP employs an AI-based neural network model for credit scoring. If a consumer questions the reason behind a low credit score, the model can explain it using reasons that emerge directly from the model that generated the score. For example, Consumer X is denied his/her credit application from a lender. In response, the consumer asks for the reasoning behind the denial. The consumer is provided with an explanation that "the number of accounts with a credit balance, number of occurrences for 30 days delinquency, age of bankcard accounts, and lack of retail accounts are listed, respectively, as the four most important factors that cause the consumer to lose points in the credit score." If the loan officer

wants to understand why Consumer X's credit application was denied, compared to similar applications from other customers, the loan officer is provided with a response such as: "Consumers A, B, and C have similar financial profiles with Consumer X, regarding their number of accounts with a credit balance, delinquency occurrences with 30 days, and age of bankcard accounts. These consumers all defaulted on their lines of credit in the last 12 months; therefore the model recommends that Consumer X's application should be denied for the time being."

Use Case 5: Security and Robustness

The CRSP established a sound data security framework under which potential vulnerabilities are regularly assessed. Preventive measures are in place to ensure the integrity and resilience of data against potential attacks. Business continuity and contingency plans are established to deal with cyber incidents. The CRSP assesses the possibility that its AI/ML systems will harm data subjects, providers, users, or other relevant third parties through any type of unintentional behavior or unintended results because of cyber vulnerabilities such as cyberattacks, data poisoning, or adversarial attacks. When adopting new technologies, appropriate due diligence is conducted, and governance mechanisms are established. Ongoing employee training programs are in place to raise awareness of and knowledge regarding information security.

Use Case 6: Lawfulness

The CRSP applies a data governance framework for the lawful collection of alternative data. The framework provides clear policies and processes on issues such as obtaining consumers' consent to collect and process data where necessary; ensuring the accuracy, currency, and validity of data collected through third-party providers; protecting the dignity and privacy of data subjects; ensuring the relevance of data for the purpose specified for its collection; and enabling consumers to access and correct their information where appropriate.

Use Case 7: Privacy

The CRSP established a data governance framework that includes a data privacy officer responsible for protecting the privacy of data subjects. Relevant technical standards such as those of ISO and IEEE are adopted for data management. Oversight mechanisms are in place for data collection, storage, processing, and use. In particular, the AI/ML system's data collection process is appropriately managed to ensure the models are trained using minimal personal data. In addition, appropriate measures, such as encryption, anonymization, and aggregation, are used to enhance personal data privacy.

The CRSP uses a blockchain-based data management platform to produce credit reports. The platform allows consumers' digital identities to be kept with relevant data. To ensure personal data privacy, the CRSP employs technologies such as secure multi-party computation to create a barrier between the consumer's identification data and all anonymized data related to that consumer.

Use Case 8: Sustainability and Well-Being

The CRSP integrates environmental, social, and governance factors into its technology practices. Sustainability principles are disclosed and incorporated into corporate strategies, policies, and processes. Credit reporting activities are pursued in line with sustainable development objectives. The CRSP highlights its environmental and social commitments compared to a set of globally recognized standards and environmental, social, and governance impact factors. In particular, the CRSP has established policies to measure both the environmental impact and the broader social impacts of the technologies employed for its credit reporting activities.

Appendix A

Additional Examples of Guidance on Responsible Technology Use in Credit Reporting

Big Data

The European Economic and Social Committee explored the ethical dimensions of Big Data in an attempt to balance them with the need for economic growth within the EU. The report identified a range of ethical issues involving awareness, control, trust, ownership, surveillance and security, digital identity, tailored reality, de-anonymization, digital divide, and privacy. In response, five balancing actions were suggested to benefit from the use of Big Data while addressing ethical considerations. The five actions can be summarized as follows:

1. Establish a privacy management platform that allows natural persons to control their own personal data.
2. Institute an ethical data management protocol to increase transparency and make people aware of big data holders' level of compliance with relevant law, both public and private.
3. Develop a data management statement to boost the confidence of internal and external stakeholders that organizations may submit to declare how they collect, use, or sell personal data from customers and general business activities.
4. Promote digital education on big data to create a broader digital culture in Europe, specifically aimed at deepening understanding of big data, how it interacts with citizens throughout their lives, and how it affects each individual.
5. Create an e-health database.

The GSM Association (GSMA) published the report, "Mobile Big Data Analytics and AI for a Better Future." The document outlines the following principles for harnessing trustworthy AI in big data analytics by ensuring its ethical use:

1. Do no harm.
2. Be inclusive.
3. Be fair.
4. Ensure transparency.
5. Embed accountability.
6. Adopt privacy and ethics by design.
7. Advance security and safety.
8. Support sustainability and societal well-being.

Open APIs

The Consultative Group to Assist the Poor (CGAP) issued a guidance note that provides key considerations when developing legal terms and conditions for financial services APIs. The document highlights the key risks and legal issues arising for various API use cases and considers how the risks could be managed through contract design and implementation. The guidance note covers the following considerations:

1. Partner selection, due diligence, and onboarding
2. Termination or suspension of access following onboarding
3. Access to APIs, obtaining consumer consent
4. Methods of authenticating the customer
5. Data protection concerns
6. Security concerns such as risks of screen-scraping
7. Allocation of liability risk
8. Technical standards
9. Licenses, dispute resolution, and business continuity/ contingency

AI/ML

The European Commission's High-Level Expert Group on AI presented its "Ethics Guidelines for Trustworthy Artificial Intelligence." The document provides guidance on how trustworthy AI can be realized under seven principles.

1. Human agency and oversight: Fundamental rights, human agency, and human oversight.
2. Technical robustness and safety: Security and resilience to attack; fall back plan; and general safety, accuracy, reliability, and reproducibility.
3. Privacy and data governance: Respect for privacy, quality and integrity of data, and access to data.
4. Transparency: Traceability, explainability, and communication.
5. Diversity, non-discrimination, and fairness: The avoidance of unfair bias, accessibility and universal design, and stakeholder participation.
6. Environmental and societal well-being: Sustainability and environmental friendliness; social impact; society

and democracy.
7. Accountability: Auditability, minimization, and reporting of negative impact, trade-offs, and redress.

Germany's Financial Supervisory Authority (BaFin) issued principles for the use of algorithms in decision-making processes. BaFin sets out as key principles clear management responsibility, appropriate risk, and outsourcing management; preventing bias; and ruling out types of differentiation prohibited by law. The guide follows these specific principles for the AI development phase:

1. Maintain data strategy and governance.
2. Comply with data protection requirements.
3. Ensure accurate, robust, and reproducible results.
4. Document systems to ensure clarity for both internal and external parties.
5. Follow appropriate validation processes.
6. Use relevant data for calibration and validation purposes.

BaFin sets out the following principles for the AI application phase:

1. Put humans in the loop.
2. Establish in-depth approval and feedback processes.
3. Establish contingency measures.
4. Conduct ongoing validation and overall evaluation and make appropriate adjustments.

Likewise, the Hong Kong Monetary Authority (HKMA) issued high-level principles on the use of AI and big data analytics. HKMA emphasizes applying the principles in a proportionate manner that reflects the nature of AI use cases and the level of risks involved. The HKMA principles include the following key considerations:

1. Governance: Accountability of the board and senior management for the outcome of AI applications.
2. Application design and development: Possessing sufficient expertise; ensuring an appropriate level of explainability of AI applications; using data of good quality; conducting rigorous model validation; ensuring auditability of AI applications; implementing effective management oversight of third-party vendors; and being ethical, fair, and transparent.
3. Ongoing monitoring and maintenance: Conducting periodic reviews and ongoing monitoring; complying with data protection requirements; implementing effective cybersecurity measures; and maintaining risk mitigation and contingency plans.

The Recommendation on AI is the first intergovernmental standard on AI adopted by the OECD. The document aims to foster innovation and trust in AI by promoting responsible stewardship of trustworthy AI and ensuring respect for human rights and democratic values. The document identifies five complementary values-based principles for the responsible stewardship of trustworthy AI and calls on stakeholders to promote and implement these principles:

1. Inclusive growth, sustainable development, and well-being
2. Human-centered values and fairness
3. Transparency and explainability
4. Robustness, security and safety
5. Accountability

The Institute of Electrical and Electronics Engineers (IEEE) issued principles for ethically aligned design as part of its vision for Prioritizing Human Well-Being with Autonomous and Intelligent Systems. The document advises on the following principles:

1. Human Rights
2. Prioritizing Well-Being
3. Accountability
4. Transparency
5. Technology Misuse and Awareness

Digital ID & Biometrics

The UN published the "Compendium of Recommended Practices for the Responsible Use and Sharing of Biometrics in Counter-Terrorism." While the compendium primarily addresses state authorities, the following recommendations are relevant for the responsible use of biometrics:

1. Adopt a human-rights based approach that includes procedural safeguards and effective oversight of applications. Establish or expand independent, appropriate oversight bodies to supervise implementing relevant privacy legislation and providing effective remedies in case of violations, to be supplemented by an ethical review process.
2. Conduct regular risk assessments of the end-to-end processes of biometric applications against cyber threats and vulnerabilities.
3. Assure the compliance of biometric systems with international technical standards to ensure meeting business needs in terms of accuracy, security, and operational reliability.

WEF developed a Framework for Action for Responsible Limits on Facial Recognition (WEF 2020c). The goal of the initiative is to establish a governance framework for facial recognition technology, recommending the following principles for organizations taking action:

1. Take appropriate steps to ensure that unfair bias or outcomes can be detected.
2. Take reasonable steps to assess the capabilities for use and limitations of the systems and ensure systems are appropriate for purpose.
3. Design systems to support privacy, including privacy considerations in system requirements and carrying through privacy support in the design, development, and testing of technology.
4. Ensure a culture of accountability internally and across third-party service providers or business partners.
5. Conduct a comprehensive risk assessment of systems, including the impact on privacy, potential for errors, susceptibility to unfair bias, vulnerability to hacking and cyberattacks, lack of transparency in the decision-making process, and potential for civil rights infringements.
6. Follow the standards for evaluating the accuracy and performance of systems at the design (lab tests) and deployment (field tests) stages.
7. Provide information to end users who have questions and/or need information on the use of systems.
8. Obtain informed, explicit, affirmative consent from individuals for the use of systems.
9. Ensure facial recognition does not exclude anyone and is always accessible to and usable by all groups of people, including elderly people and people with disabilities.
10. Conduct human oversight for any use that could result in a consequential decision, such as an infringement of a civil right.

Cloud Computing

The European Banking Authority (EBA) published recommendations on outsourcing to cloud service providers to clarify the EU-wide supervisory expectations for institutions intending to adopt cloud computing. The recommendations were calibrated to allow the institutions to leverage the benefits of using cloud services while ensuring that any related risks are adequately identified and managed. The document covers the following topics:

1. Conducting materiality assessment
2. Duty to adequately inform supervisors
3. Determination of access and audit rights
4. Security of data and systems
5. Considerations on the location of data and data processing
6. Managing risks associated with chain outsourcing
7. Contingency plans and exit strategies

Distributed Ledger Technologies

Gibraltar Financial Services Commission issued the following regulatory principles to be applied by DLT providers:

1. Conduct business with honesty and integrity.
2. Pay due regard to the interests and needs of each and all customers, and communicate with customers in a way that is fair, clear, and not misleading.
3. Maintain adequate financial and nonfinancial resources.
4. Manage and control business effectively and conduct business with due skill, care, and diligence, including having proper regard to risks to the business and its customers.
5. Establish effective arrangements for the protection of clients' assets and money.
6. Have effective corporate governance arrangements.
7. Ensure that all systems and security access protocols are maintained to appropriate high standards.
8. Have systems in place to prevent, detect, and disclose financial crime risks such as money laundering and terrorist financing.
9. Be resilient and develop contingency plans for the orderly, solvent wind-down of business.

Appendix B

Glossary

Term	Definition	Source
Alternative credit reporting service provider	Entities that use innovative methodologies and nontraditional data to assess credit risk and produce credit scores.	Authors
Artificial intelligence	The theory and development of computer systems able to perform tasks that traditionally have required human intelligence.	FSB (2017)
Big data	A generic term that designates the massive volume of data generated by the increasing use of digital tools and information systems.	FSB (2017)
Business information provider	Entities that collect information on businesses, including sole proprietorships, partnerships, and corporations for credit risk assessment, credit scoring, or other business purposes.	World Bank (2011)
Code of conduct	A self-regulatory framework for credit reporting service providers that governs their relationship to data providers, users, borrowers, other bureaus, and the supervisory authority.	Authors
Consumer	See data subject.	
Consumer consent	A data subject's freely informed, specific agreement, written or verbal, to the collection, processing, and disclosure of personal data.	World Bank (2011)
Credit bureau	Model of a credit-information exchange the primary objective of which is to improve the quality and availability of data so creditors can make better-informed decisions.	World Bank (2011)
Credit registry	Model of a credit-information exchange the main objectives of which are assisting prudential supervision and enabling data access to regulated financial institutions to improve the quality of their credit portfolios.	World Bank (2011)
Credit reporting service provider	Entities that collect information on a borrower's credit history from creditors and available public sources; includes credit bureaus, credit registries, business information providers, and alternative credit reporting service providers.	World Bank (2019a)
Credit risk	The risk that a counterparty will fail to make any of the payments that it is contractually obliged to make.	ECB (2018)
Credit score	Form of statistical analysis that estimates the probability that a loan applicant, existing borrower, or counterparty will default or become delinquent.	ICCR (2019a)
Creditworthiness	The ability of a borrower to repay current and prospective financial obligations in a timely manner; used as an assessment of a borrower's past credit behavior to assist a potential lender in deciding whether to extend new credit.	World Bank (2011)
Data provider	A creditor or other entity that proactively and in a structured fashion supplies information to the credit reporting service providers.	World Bank (2011)
Data subject	An individual or a business whose data could be collected, processed, and disclosed to third parties in a credit reporting system.	World Bank (2011)
Data user	An individual or business that requests credit reports, files, or other related services from credit reporting service providers, typically under predefined conditions and rules.	World Bank (2011)

Default	Failure to complete a payment obligation under a credit or loan agreement.	World Bank (2011)
IaaS	Infrastructure as a service; a cloud service provider's ability to provision processing, storage, networks, and other fundamental computing resources where the customer can deploy and run arbitrary software.	NIST (2017b)
Machine learning	A method of designing a sequence of actions to solve a problem in a way that optimizes automatically through iteration, with limited or no human intervention.	FSB (2017)
Negative information	Statements about defaults or arrears and bankruptcies; may also include statements about lawsuits, liens, and judgments obtained from courts or other official sources.	World Bank (2011)
PaaS	Platform as a service; a software development and/or deployment platform with the capability to develop and/or deploy applications without the complexities of managing underlying infrastructure services.	NIST (2017b)
Permissioned	Requiring authorization to perform a particular activity or activities.	ITU (2019a)
Permissionless	Not requiring authorization to perform a particular activity.	ITU (2019a)
Personal data	Information relating to an identified or identifiable natural person ("data subject"); an identifiable person is one who can be identified, directly or indirectly, in particular by reference to an ID number or one or more factors specific to the person's physical, physiological, mental, economic, cultural, or social identity.	ICCR (2021)
Positive information	Information that covers facts of contractually compliant behavior, including detailed statements about outstanding credit, amount of loans, repayment patterns, assets, liabilities, and guarantees and/or collateral.	World Bank (2011)
RegTech	Any range of applications of fintech for regulatory and compliance requirements and reporting by regulated financial institutions.	FSB (2017)
SaaS	Software as a service; services in which the customer can use the cloud service provider's applications running on a cloud infrastructure; applications are accessible through either a thin client interface, such as a web browser, or a program interface.	NIST (2017b)
Structured data	Any data that reside in a fixed field within a record or file. Typically, the data reside in the form of relational databases and spreadsheets. The formal structure allows one to easily enter, store, query, and analyze the data.	ICCR (2019a)
Supervised learning	A subset of machine learning in which an algorithm is fed a set of "training" data that contains labels on the observations.	FSB (2017)
SupTech	Applications of fintech by supervisory authorities.	FSB (2017)
Unstructured data	Data that do not have a predefined data model or are not organized in a predefined manner; they typically exist in the form of text files, images, social media data, and sensor data.	ICCR (2019a)
Unsupervised learning	A subset of machine learning in which the data provided to the algorithm does not contain labels.	FSB (2017)

Appendix C

Bibliography

Akinwumi, M., J. Merrill, L. Rice, K. Saleh, and M. Yap. 2021. "An AI Fair Lending Policy Agenda for the Federal Financial Regulators." Series on Financial Markets and Regulation, Brookings Institution, Washington, DC. https://www.brookings.edu/research/an-ai-fair-lending-policy-agenda-for-the-federal-financial-regulators/.

Aldasoro, I., L. Gambacorta, P. Giudici, and T. Leach. 2020. "The Drivers of Cyber Risk." BIS Working Papers No. 865, Bank for International Settlements, Basel, Switzerland. https://www.bis.org/publ/work865.pdf.

BaFin (Bundesanstalt für Finanzdienstleistungsaufsicht). 2021. "Big Data and Artificial Intelligence: Principles for the Use of Algorithms in Decision-Making Processes." Federal Financial Supervisory Authority, Bonn, Germany. https://www.bafin.de/SharedDocs/Downloads/EN/Aufsichtsrecht/dl_Prinzipienpapier_BDAI_en.html.

Basel Committee on Banking Supervision (BCBS). 2019. "Implications of Fintech Developments for Banks and Bank Supervisors." Bank for International Settlements. https://www.bis.org/bcbs/publ/d431.pdf

Berg, T., V. Burg, A. Gombović, and M. Puri. 2019. "On the Rise of FinTechs — Credit Scoring Using Digital Footprints." Michael J. Brennan Irish Finance Working Paper Series Research Paper No.18-12. http://dx.doi.org/10.2139/ssrn.3163781.

Biometrics Institute. 2019. "Ethical Principles for Biometrics." Biometrics Institute, London. https://www.biometricsinstitute.org/ethical-principles-for-biometrics/.

Bussmann, N., Giudici, P., Marinelli, D. 2021. "Explainable Machine Learning in Credit Risk Management". Computational Economics 57, 203–216 (2021). https://doi.org/10.1007/s10614-020-10042-0

Calmon, F., D. Wei, B. Vinzamuri, K. Natesan Ramamurthy, and K. R. Varshney. 2017. "Optimized Pre-Processing for Discrimination Prevention." Advances in Neural Information Processing Systems 30. 31st Conference on Neural Information Processing Systems (NIPS 2017), Long Beach, CA. https://papers.nips.cc/paper/2017/hash/9a49a25d845a483fae4be7e341368e36-Abstract.html. Last accessed June 9, 2021.

Centre for Data Ethics and Innovation (CDEI). 2020. "Review into Bias in Algorithmic Decision-making." Centre for Data Ethics and Innovation, London. https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/957259/Review_into_bias_in_algorithmic_decision-making.pdf.

CGAP (Consultative Group to Assist the Poor). 2020. "Guidance Note: Key Considerations When Developing Legal Terms and Conditions for Financial Services APIs." CGAP, World Bank, Washington, DC. https://www.findevgateway.org/sites/default/files/publications/files/cgap-guidance-note-key-considerations-when-developing-legal-terms-and-conditions-for-financial-services-apis-january-2020.pdf.

Creditinfo. 2020. "Global Lending Industry Trends." CreditInfo, Reykjavík, Iceland. https://creditinfo.com/wp-content/uploads/2017/08/creditinfo_trends_2020.pdf.

CSSF (Commission de Surveillance du Secteur Financier). 2018. "AI: Opportunities, Risks and Recommendations for the Financial Sector." Commission de Surveillance du Secteur Financier, Luxembourg. https://www.cssf.lu/wp-content/uploads/files/Publications/Rapports_ponctuels/CSSF_White_Paper_Artificial_Intelligence_201218.pdf.

Data Reportal. 2021. "Global Digital Overview October 2021." Data Reportal, Singapore. https://datareportal.com/reports/digital-2021-october-global-statshot.

ECB (European Central Bank). 2018. Anacredit. European Central Bank, European Union, Paris. https://www.ecb.europa.eu/stats/money_credit_banking/anacredit/html/index.en.html.

Equifax. 2020a. "Putting Neural Network Models to the Test." Equifax, Atlanta, GA. https://www.equifax.com/white-papers/putting-neural-network-models-test/.

Equifax. 2020b. "Seizing the Cloud Opportunity — Securely and Safely." Equifax, Atlanta, GA. https://assets.equifax.com/marketing/US/assets/equifax_seizing_cloud_opportunity_safely_security_paper_aug2020.pdf. Last accessed Jan. 31, 2022.

Equifax. 2021. "Equifax Data Breach Settlement." Equifax, Atlanta, GA. https://www.equifaxbreachsettlement.com/. Last accessed June 24, 2021.

EU (European Union). 2016. "General Data Protection Regulation." European Union, Brussels. https://gdpr-info.eu/.

EU (European Union). 2021. "Proposal for a Regulation of the European Parliament and of the Council Laying Down Harmonized Rules on Artificial Intelligence (Artificial Intelligence Act) and Amending Certain Union Legislative Acts." European Union, Brussels. https://eur-lex.europa.eu/legal-content/EN/TXT/?qid=1623335154975&uri=CELEX%3A52021PC0206.

European Banking Authority (EBA). 2020. "EBA Report on Big Data and Advanced Analytics." European Banking Authority, Paris. https://www.eba.europa.eu/sites/default/documents/files/document_library/Final%20Report%20on%20Big%20Data%20and%20Advanced%20Analytics.pdf.

"Experian Enables Next Generation Data Analytics Platform Using AWS." Experian, Costa Mesa, CA. https://aws.amazon.com/tr/solutions/case-studies/experian/. Last accessed Jan. 31, 2022.

Federal Deposit Insurance Corporation (FDIC). 2017. "Supervisory Guidance on Model Risk Management." Federal Deposit Insurance Corporation, Washington, DC. https://www.fdic.gov/news/financial-institution-letters/2017/fil17022a.pdf.

Fjeld, J., A. Nele, H. Hilligoss, A. Nagy, and M. Srikumar. 2020. "Principled Artificial Intelligence: Mapping Consensus in Ethical and Rights-based Approaches to Principles for AI." Berkman Klein Center for Internet and Society, Harvard University, Cambridge, MA. https://dash.harvard.edu/bitstream/handle/1/42160420/HLS%20White%20Paper%20Final_v3.pdf?sequence=1&isAllowed=y.

Frost, J., L. Gambacorta, Y. Huang, H. S. Shin, and P. Zbinden. 2019. "BigTech and the Changing Structure of Financial Intermediation." BIS Working Papers No. 779, Bank for International Settlements, Basel, Switzerland. https://www.bis.org/publ/work779.pdf.

FSB (Financial Stability Board). 2017. "Artificial Intelligence and Machine Learning in Financial Services — Market Developments and Financial Stability Implications." Financial Stability Board, Basel, Switzerland. https://www.fsb.org/wp-content/uploads/P011117.pdf. Last accessed June 9, 2022.

Gambacorta, L., Y. Huang, and J. Wang. 2019. "How do ML and non-traditional data affect credit scoring? New Evidence from a Chinese Fintech Firm." BIS Working Papers No. 834. Bank for International Settlements, Basel, Switzerland. https://www.bis.org/publ/work834.pdf.

Gauthier, J. 2009. "Ethical principles and human rights: Building a better world globally." Counselling Psychology Quarterly 22:1, 25–32. https://www.tandfonline.com/doi/abs/10.1080/09515070902857301.

Gibraltar Financial Services Commission. 2020. "The Regulatory Principles for DLT Providers." Gibraltar Financial Services Commission, Gibraltar. https://www.fsc.gi/FSC/distributed-ledger-technology-providers.

Goharshady, A. Behrouz A. and Chatteriee K. 2018. "Secure Credit Reporting on the Blockchain." 2018 IEEE International Conference, pp. 1343-1348. https://ieeexplore.ieee.org/document/8726769

GSM Association (GSMA). 2019a. "Mobile Big Data Analytics and AI for a Better Future: AI Ethics Principles." GSMA, London. https://www.gsma.com/betterfuture/wp-content/uploads/2019/09/AI-Ethics_2Pager_v1.pdf.

GSM Association (GSMA). 2019b. "Mobile Big Data Solutions for a Better Future Report." GSMA, London. https://www.gsma.com/betterfuture/wp-content/uploads/2019/10/2019-GSMA-Mobile-Big-Data-for-a-Better-Future_Full-Report-1.pdf.

GPFI. 2017. "Alternative Data Transforming SME Finance." https://www.gpfi.org/sites/gpfi/files/documents/GPFI%20Report%20Alternative%20Data%20Transforming%20SME%20Finance.pdf and and https://www.smefinanceforum.org/post/alternative-data-transforming-sme-finance-0 and https://www.gpfi.org/publications/gpfi-report-alternative-data-transforming-sme-finance

Hagendorff, T. 2020. "The Ethics of AI Ethics: An Evaluation of Guidelines." Minds and Machines 30:99–120. https://doi.org/10.1007/s11023-020-09517-8.

Hengel, E. 2010. "Discussion Paper on Credit Information Sharing." Facilitating Access to Finance Discussion Paper Series, Organization for Economic Co-operation and Development, Paris. https://www.oecd.org/global-relations/45370071.pdf.

Hong Kong Monetary Authority (HKMA). 2019. "High-Level Principles on AI." Hong Kong Monetary Authority, Hong Kong. https://www.hkma.gov.hk/media/eng/doc/key-information/guidelines-and-circular/2019/20191101e1.pdf.

Hyperledger Case Study — Kiva. Hyperledger Foundation. https://www.hyperledger.org/wp-content/uploads/2021/01/Hyperledger_CaseStudy_Kiva_Printable.pdf.
Last accessed Jan. 31, 2022.

IBM. Trusted AI Tools. International Business Machines, Armonk, NY. https://research.ibm.com/teams/trusted-ai. Last accessed Jan. 31, 2022.

ICCR (International Committee on Credit Reporting). 2013. "Assessment Methodology for the General Principles for Credit Reporting." ICCR, World Bank, Washington, DC.
http://hdl.handle.net/10986/21813.

ICCR (International Committee on Credit Reporting). 2014. "Facilitating SME Financing through Improved Credit Reporting." ICCR, World Bank, Washington, DC. http://hdl.handle.net/10986/21810.

ICCR (International Committee on Credit Reporting). 2018. "Use of Alternative Data to Enhance Credit Reporting to Enable Access to Digital Financial Services by Individuals and SMEs Operating in the Informal Economy." Global Partnership for Financial Inclusion Guidance Note. ICCR, World Bank, Washington DC. https://www.gpfi.org/sites/gpfi/files/documents/Use_of_Alternative_Data_to_Enhance_Credit_Reporting_to_Enable_Access_to_Digital_Financial_Services_ICCR.pdf.

ICCR (International Committee on Credit Reporting). 2019a. "Credit Scoring Approaches Guidelines" ICCR, World Bank, Washington, DC. https://thedocs.worldbank.org/en/doc/935891585869698451-0130022020/original/CREDITSCORINGAPPROACHESGUIDELINESFINALWEB.pdf.

ICCR (International Committee on Credit Reporting). 2019b. "Cybersecurity in Credit Reporting Guidelines." ICCR, World Bank, Washington, DC. https://thedocs.worldbank.org/en/doc/735641585870130697-0130022020/original/Cybersecurityincreditreportingguidelinefinal.pdf.

International Committee on Credit Reporting (ICCR). 2021. "Cross-border Credit Reporting" World Bank, Washington, DC. https://www.biia.com/wp-content/uploads/2021/08/ICCR-Cross-Border-Report-final-July-2021.pdf

IEEE Global Initiative on Ethics of Autonomous and Intelligent Systems. 2017. "Ethically Aligned Design: A Vision for Prioritizing Human Well-being with Autonomous and Intelligent Systems." Institute of Electrical and Electronics Engineers, New York. http://standards.ieee.org/develop/indconn/ec/autonomous_ systems.html.

International Organization of Securities Commissions (IOSCO). 2021. "Principles on Outsourcing." International Organization of Securities Commissions, Madrid. https://www.iosco.org/library/pubdocs/pdf/IOSCOPD687.pdf.

ITU (International Telecommunication Union). 2019a. "Distributed Ledger Technology Terms and Definitions." International Telecommunication Union, Geneva, Switzerland. https://www.itu.int/en/ITU-T/focusgroups/dlt/Documents/d11.pdf. Last accessed June 9, 2022.

ITU (International Telecommunication Union). 2019b. "Technical Report — Distributed Ledger Technology Framework." International Telecommunication Union, Geneva, Switzerland. https://www.itu.int/en/ITU-T/focusgroups/dlt/Documents/d41.pdf. Last accessed June 9, 2022.

Liu, C., and C. Hou. 2021. "Challenges of Credit Reference Based on Big Data Technology in China." Mobile Networks and Applications 27:47–57 (2022). https://doi.org/10.1007/s11036-020-01708-y.

MAS (Monetary Authority of Singapore). 2018. "Principles to Promote Fairness, Ethics, Accountability and Transparency (FEAT) in the Use of Artificial Intelligence and Data Analytics in Singapore's Financial Sector." Monetary Authority of Singapore, Singapore. https://www.mas.gov.sg/~/media/MAS/News%20and%20Publications/Monographs%20and%20Information%20Papers/FEAT%20Principles%20Final.pdf.

National Fair Housing Alliance (NFHA). 2022. "Purpose, Process and Monitoring: A New Framework in Auditing Algorithmic Bias in Housing & Lending." National Fair Housing Alliance, Washington, DC. https://nationalfairhousing.org/wp-content/uploads/2022/02/PPM_Framework_02_17_2022.pdf. Last accessed June 9, 2022.

National Telecommunications and Information Administration (NTIA). N.d. "An Ethical Framework for Facial Recognition." National Telecommunications and Information Administration, Washington, DC. https://www.ntia.doc.gov/files/ntia/publications/aclu_an_ethical_framework_for_face_recognition.pdf.

NIST (National Institute of Standards and Technology). 2017a. "Cybersecurity Framework." National Institute of Standards and Technology, Gaithersburg, MD, and Boulder, CO. https://nvlpubs.nist.gov/nistpubs/ir/2017/NIST.IR.8183.pdf.

NIST (National Institute of Standards and Technology). 2017b. "Draft — Evaluation of Cloud Computing Services Based on NIST 800-145." National Institute of Standards and Technology, Gaithersburg, MD, and Boulder, CO. https://www.nist.gov/system/files/documents/2017/05/31/evaluation_of_cloud_computing_services_based_on_nist_800-145_20170427clean.pdf.

NIST (National Institute of Standards and Technology). 2021. "AI Risk Management Framework Concept Paper." National Institute of Standards and Technology, Gaithersburg, MD, and Boulder, CO. https://www.nist.gov/system/files/documents/2021/12/14/AI%20RMF%20Concept%20Paper_13Dec2021_posted.pdf.

OBIE (Open Banking Implementation Entity). N.d. "Customer Experience Standards." Open Banking Implementation Entity, U.K. https://standards.openbanking.org.uk/customer-experience-guidelines/introduction/design-and-experience-principles/latest/. Last accessed Jan. 31, 2022.

OneScore Mobile App by Experian India. N.d. OneScore, Pune.
https://www.onescore.app/. Last accessed Jan. 31, 2022.

Open Technology Institute. 2021. "Cracking Open the Black Box: Promoting Fairness, Accountability, and Transparency Around High-Risk AI." Open Technology Institute, Washington, DC. https://www.newamerica.org/oti/reports/cracking-open-the-black-box/.

Organization for Economic Co-operation and Development (OECD). 2019. "Recommendation of the Council on Artificial Intelligence." Organization for Economic Co-operation and Development, Paris. https://legalinstruments.oecd.org/en/instruments/OECD-LEGAL-0449.

Singapore Personal Data Protection Commission. 2020. "Model AI Governance Framework." Singapore Personal Data Protection Commission, Singapore. https://www.pdpc.gov.sg/-/media/Files/PDPC/PDF-Files/Resource-for-Organisation/AI/SGModelAIGovFramework2.pdf.

Singapore Personal Data Protection Commission. 2020. "Compendium of Use Cases: Practical Illustrations of the Model AI Governance Framework." Singapore Personal Data Protection Commission, Singapore. https://www.pdpc.gov.sg/-/media/Files/PDPC/PDF-Files/Resource-for-Organisation/AI/SGAIGovUseCases.pdf.

Toronto Centre. 2018. "Cloud Computing: Issues for Supervisors." TC Notes. Toronto Centre, Toronto. https://res.torontocentre.org/guidedocs/Risk-Based%20Supervision%20FINAL.pdf.

TransUnion. 2021. "TransUnion and AWS Executives Explores How Disruptive Work Flows Unlock Banking Opportunities." TransUnion, Chicago, IL. https://www.globenewswire.com/news-release/2021/09/30/2306150/0/en/Panel-with-TransUnion-and-AWS-Executives-Explores-How-Disruptive-Work-Flows-Unlock-Banking-Opportunities.html. Last accessed Jan. 31, 2022.

UN (United Nations). 2011. "Guiding Principles on Business and Human Rights." United Nations, New York. https://www.ohchr.org/documents/publications/guidingprinciplesbusinesshr_en.pdf.

UN (United Nations). 2017. "Data Privacy, Ethics and Protection: Guidance Note on Big Data for Achievement of the 2030 Agenda." United Nations, New York. https://unsdg.un.org/resources/data-privacy-ethics-and-protection-guidance-note-big-data-achievement-2030-agenda.

UN (United Nations). 2018. "Compendium of Recommended Practices for the Responsible Use and Sharing of Biometrics in Counter-Terrorism." United Nations, New York. https://www.un.org/securitycouncil/ctc/sites/www.un.org.securitycouncil.ctc/files/files/documents/2021/Jan/compendium_on_biometricsl_eng.pdf.

UN (United Nations). 2021. "Resource Guide on AI Strategies." United Nations, New York. https://sdgs.un.org/sites/default/files/2021-04/Resource%20Guide%20on%20AI%20Strategies_April%202021_rev_0.pdf.

UN (United Nations). 2022. "Digital Space and Human Rights". United Nations, New York. https://www.ohchr.org/en/topic/digital-space-and-human-rights. Last accessed Jan. 31, 2022.

UNESCO (United Nations Educational, Scientific and Cultural Organization). 2021. "Recommendations on the Ethics of AI." UNESCO, Paris. https://en.unesco.org/artificial-intelligence/ethics#recommendation.

Veritas Consortium. 2020. "FEAT Fairness Principles Assessment Case Studies." Monetary Authority of Singapore, Singapore. https://www.mas.gov.sg/-/media/MAS/News/Media-Releases/2021/Veritas-Document-1-FEAT-Fairness-Principles-Assessment-Methodology.pdf.

Veritas Consortium. 2021. "FEAT Fairness Principles Assessment Case Studies." Monetary Authority of Singapore, Singapore. https://www.mas.gov.sg/-/media/MAS/News/Media-Releases/2021/Veritas-Document-2-FEAT-Fairness-Principles-Assessment-Case-Studies.pdf.

WEF (World Economic Forum). 2018. "Responsible Use of Technology." World Economic Forum, Cologny, Switzerland. https://www3.weforum.org/docs/WEF_Responsible_Use_of_Technology.pdf.

WEF (World Economic Forum). 2020a. "Companion to the AI Model Governance Framework – Implementation and Self-Assessment Guide for Organizations." World Economic Forum, Cologny, Switzerland. https://www.pdpc.gov.sg/-/media/

Files/PDPC/PDF-Files/Resource-for-Organisation/AI/SGIsago.pdf.

WEF (World Economic Forum). 2020b. "Ethics by Design: An Organizational Approach to Responsible Use of Technology." World Economic Forum, Cologny, Switzerland. https://www3.weforum.org/docs/WEF_Ethics_by_Design_2020.pdf.

WEF (World Economic Forum). 2020c. "A Framework for Responsible Limits on Facial Recognition Use Case: Flow Management." World Economic Forum, Cologny, Switzerland. https://www3.weforum.org/docs/WEF_Framework_for_action_Facial_recognition_2020.pdf.

WEF (World Economic Forum). 2021. "Responsible Use of Technology: The IBM Case Study." World Economic Forum, Cologny, Switzerland. https://www3.weforum.org/docs/WEF_Responsible_Use_of_Technology_The_IBM_Case_Study_2021.pdf.

World Bank. 2011. "General Principles for Credit Reporting." World Bank, Washington DC. http://hdl.handle.net/10986/12792.

World Bank. 2018. "Improving Access to Finance for SMEs: Opportunities through Credit Reporting, Secured Lending and Insolvency Practices." World Bank, Washington, DC. https://documents1.worldbank.org/curated/en/316871533711048308/pdf/129283-WP-PUBLIC-improving-access-to-finance-for-SMEs.pdf

World Bank Group. 2019a. "Credit Reporting Knowledge Guide 2019." World Bank, Washington, DC. http://hdl.handle.net/10986/31806.

World Bank Group. 2019b. "Disruptive Technologies in the Credit Information Sharing Industry: Developments and Implications." Fintech Note No. 3, World Bank, Washington, DC. http://hdl.handle.net/10986/31714.

World Bank. 2020. "Doing Business 2020: Comparing Business Regulation in 190 Economies." World Bank, Washington, DC. http://hdl.handle.net/10986/32436.

World Bank. 2021a. "Consumer Risks in Fintech: New Manifestations of Consumer Risks and Emerging Regulatory Approaches." World Bank, Washington, DC. http://hdl.handle.net/10986/35699.

World Bank. 2021b. "Principles on Identification for Sustainable Development." World Bank, Washington, DC. https://id4d.worldbank.org/principles.

World Bank and CGAP (Consultative Group to Assist the Poor). 2018. "Data Protection and Privacy for Alternative Data." Global Partnership for Financial Inclusion Discussion Paper, World Bank, Washington, DC. https://www.gpfi.org/sites/gpfi/files/documents/Data_Protection_and_Privacy_for_Alternative_Data_WBG.pdf.

Yong, J., Prenio, J. 2021. "Humans Keeping AI in Check: Emerging Regulatory Expectations in the Financial Sector." FSI Insights on Policy Implementation No. 35, Bank for International Settlements, Basel, Switzerland. https://www.bis.org/fsi/publ/insights35.pdf.

Reference

[1]. The members of the West African Economic and Monetary Union (also known by its French acronym, UEMOA) are Benin, Burkina Faso, Côte D'Ivoire, Guinea-Bissau, Mali, Niger, Senegal, and Togo.

WORLD BANK GROUP