HONG KONG MONETARY AUTHORITY
香港金融管理局

Our Ref: B4/1C
B9/32C
B9/60C

26 March 2026

The Chief Executive
All Authorized Institutions

Dear Sir/Madam,

Consumer Protection in the Use of Alternative Data

I am writing to provide authorized institutions ("AIs") with a set of guiding principles in respect of consumer protection in the use of alternative data in banking operations (such as credit risk assessment).

Objectives

The use of alternative data in banking operations (especially in credit risk assessment but also in customer onboarding and provision of various products and services in general) is increasingly prevalent. This is attributable to the rapid digitalisation and technological advancements which have expanded the availability of alternative data sources and computational power for data analytics.

The distinction between traditional credit data and alternative data lies primarily in the source and type of information used to assess a borrower's creditworthiness. In general, traditional credit data refers to credit and financial information focusing on borrowers' debt history and repayment record, typically maintained by credit reference agencies ("CRAs"), which reflect borrowers' ability and willingness to repay based on their historical credit activity. Alternative data, on the other hand, encompasses a vast range of non-traditional and often non-credit-related information sources that are not part of standard reports from CRAs. This type of data can reveal patterns, trends, or signals indicative of a borrower's financial capacity that is typically not captured by traditional sources, including transactional

data (e.g. utility payment and e-commerce data), and non-transactional data (e.g. behavioural, social media and Web data).

While traditional credit data remains a core component of credit risk assessment, CRAs and other data service providers are introducing alternative data products and solutions for credit providers in support of credit risk assessments, complementing the use of traditional credit data. This integrated approach in the use of traditional and alternative data provides more comprehensive information about the background and financial situations of customers and borrowers, enabling a more complete and real-time view of borrowers' risk profiles and facilitating the evaluation of borrowers who may be excluded by traditional methods due to a lack of sufficient reliable traditional credit histories, thereby broadening the scope of credit risk assessment.

Meanwhile, international standards and recommendations on the responsible use of alternative data in financial services are emerging and evolving. In drawing up the supervisory requirements and expectations, the Hong Kong Monetary Authority ("HKMA") has made reference to international experiences and best practices, such as the World Bank report on "The Use of Alternative Data in Credit Risk Assessment: Opportunities, Risks, and Challenges" published in 2024.

Guiding principles

In general, and in line with pre-existing requirements as set out in Supervisory Policy Manual ("SPM") modules IC-6 "The Sharing and Use of Consumer Credit Data through Credit Reference Agencies" and IC-7 "The Sharing and Use of Commercial Credit Data through a Commercial Credit Reference Agency", AIs should have put in place clear and comprehensive policies and procedures governing the use of consumer and commercial credit data obtained from CRAs in managing credit risk. Such policies and procedures (including but not limited to management of service providers, access control, confidentiality and retention, compliance audit) should also apply to the use of alternative data by AIs in a technology- and source-neutral way. AIs should also enter into a formal contractual agreement with any alternative data provider(s) whose service they intend to engage, and require that data provider(s) to have effective control systems to ensure compliance with all the relevant legal and regulatory requirements.

Recognising that alternative data is generally more diverse, less standardised or structured in nature, and considering the expanding availability of data sources, the HKMA has set out some additional guiding principles, with a view to supporting AIs' ongoing innovation and enhancement of banking services to meet evolving customer needs, while strengthening consumer protection in the use of alternative data in the context of banking operations. These guiding principles on consumer

protection focus on four major areas, namely, governance and accountability, transparency and consent management, data quality and fairness, and data privacy and protection. AIs should adopt a risk-based approach commensurate with the evolving risks associated with the use of alternative data when applying these guiding principles.

1. Governance and accountability

The board and senior management of AIs should remain responsible and accountable for approving and overseeing the policies and procedures established for the use of alternative data, as well as all alternative data-driven decisions and processes. They should ensure, among others:

(a) the objectives, roles, responsibilities, and permissible data sources in the use of alternative data are clearly defined;

(b) robust and adequate data policies governing customer consent management, validation, collection, processing, correction (where applicable), and storage of alternative data are put in place;

(c) a thorough due diligence framework and processes for selecting and verifying data sources and third-party data service providers, and for deploying implementation models and decision rules are put in place;

(d) continuous monitoring and ongoing adaptation mechanisms are in place to address data biases, inaccuracies, and errors that may be introduced by alternative data;

(e) compliance audits are conducted at least annually to verify whether adequate data management practices are in place to ensure compliance with the relevant requirements regarding the use of alternative data; and

(f) appropriate guidance and regular training are provided to staff on ethical and privacy requirements pertaining to the use of alternative data.

2. Transparency and consent management

AIs should establish clear communication with customers to ensure an appropriate level of transparency regarding the use of alternative data. This includes informing customers about the types of data being used, implementation methods and limitations, and impact on outcomes, while emphasising informed consent for the collection and use of alternative data. Accordingly, they should, among others:

(a) ensure the clarity and comprehensibility of consent mechanisms employed, enabling customers to make informed decisions about their alternative data;

(b) obtain explicit prior consent from customers before collecting or using their alternative data, and clearly inform the customers about how their data is collected, processed, and used. In this connection, AIs that participate in Commercial Data Interchange (CDI) are encouraged to exchange the customer consent with the relevant alternative data provider through CDI where applicable;

(c) collect only adequate and necessary data;

(d) maintain a transparent audit trail; and

(e) ensure implementation models are highly interpretable and decisions can be explained to the customers.

3. Data quality and fairness

AIs should establish clear protocols for suitable and proportionate data validation and evaluation to ensure the quality and fairness of alternative data, as well as the accuracy and fairness of the outcomes from credit risk assessment methods and processes[1]. Accordingly, they should, among others:

(a) adopt reasonable procedures to ensure that credit risk assessment is carried out consistently using relevant, accurate, and adequate information about customers from reliable sources;

(b) consider the variability in data quality, stability, accessibility, predictive power, nuances, and associated risks across different alternative data sources; and

(c) test and monitor credit risk assessment models to prevent and correct unfair biases or disparate impacts.

[1] This circular should be read in conjunction with any applicable guidance issued and updated by the HKMA from time to time, including the guidance on credit scoring system as set out in SPM module CR-S-5 "Credit Card Business" if AIs use alternative data in credit scoring for their credit card and unsecured consumer finance business. AIs should also refer to the circular "Credit Risk Management for Personal Lending Business" dated 27 October 2022 if alternative data is used in credit risk assessments for their New Personal-Lending Portfolio.

4. Data privacy and protection

AIs should implement necessary and effective safeguards[2] to address additional privacy and cyber risks associated with the use of alternative data, given the diverse nature of alternative data sources, such as mobile phone use, text messages, geolocation and social connections of customers. Accordingly, they should, among others:

(a) ensure compliance with the requirements of the Personal Data (Privacy) Ordinance (Cap. 486);

(b) adopt all reasonable procedures (e.g. enforcing strict data security protocols, prioritising high standards of data privacy) to ensure that customers' alternative data is properly safeguarded, with regard to the security, confidentiality and proper utilisation of the data; and

(c) guard against unauthorized access to or use of private and sensitive customer information that could be vulnerable to breaches or exploitation, potentially leading to identity theft, discrimination, or other forms of harm.

Intersections of artificial intelligence and alternative data

The use of alternative data in banking operations are often coupled with the use of artificial intelligence and machine learning techniques, which can unlock the potential of alternative data by rapidly processing and identifying correlations across various structured and unstructured alternative data sources, and enabling faster credit underwriting and lending decisions. To address the relevant risks to consumers in connection with the use of artificial intelligence, AIs are reminded to refer to the HKMA circulars "Consumer Protection in respect of Use of Big Data Analytics and Artificial Intelligence by Authorized Institutions" dated 5 November 2019 and "Consumer Protection in respect of Use of Generative Artificial Intelligence" dated 19 August 2024. As a general expectation, AIs should also refer to the HKMA's circular on "High-level Principles on Artificial Intelligence" dated 1 November 2019 when adopting artificial intelligence in their operations, including for the processing of alternative data.

[2] AIs should, as appropriate, also refer to the HKMA's earlier guidance on customer data protection, including the circulars "Sound Practices for Customer Data Protection" dated 4 April 2022 and "Customer Data Protection" dated 14 October 2014.

Conclusion

AIs are expected to review and, where necessary, enhance their current policies, procedures, and practices to align with the above guiding principles. The HKMA will monitor industry developments and provide further guidance as necessary to adapt to the evolving data ecosystem and environment.

Should you have any questions regarding this circular, please contact us at credit_referencing_data@hkma.gov.hk.

Yours faithfully,

Alan Au
Executive Director (Banking Conduct)

cc: The Chairman, The Hong Kong Association of Banks
The Chairman, The DTC Association
Secretary for Financial Services and the Treasury
(Attn: Mr Timothy Wong)