SASB STANDARDS

Now part of IFRS Foundation

Consumer Finance

Sustainability Accounting Standard

FINANCIALS SECTOR

Sustainable Industry Classification System® (SICS®) FN-CF

Under Stewardship of the International Sustainability Standards Board

INDUSTRY STANDARD | VERSION 2023-12

IFRS Sustainability

sasb.org

ABOUT THE SASB STANDARDS

As of August 2022, the International Sustainability Standards Board (ISSB) of the IFRS Foundation assumed responsibility for the SASB Standards. The ISSB has committed to maintain, enhance and evolve the SASB Standards and encourages preparers and investors to continue to use the SASB Standards.

IFRS S1 *General Requirements for Disclosure of Sustainability-related Financial Information* (IFRS S1) requires entities to refer to and consider the applicability of disclosure topics in the SASB Standards when identifying sustainability-related risks and opportunities that could reasonably be expected to affect an entity's prospects. Similarly, IFRS S1 requires entities to refer to and consider the applicability of metrics in the SASB Standards when determining what information to disclose regarding sustainability-related risks and opportunities.

In June 2023, the ISSB amended climate-related topics and metrics in the SASB Standards to align them with the industry-based guidance accompanying IFRS S2 *Climate-related Disclosures*. In December 2023, the ISSB amended the non-climate-related topics and metrics in connection with the International Applicability of SASB Standards project.

Effective Date

This version 2023-12 of the Standard is effective for all entities for annual periods beginning or after January 1, 2025. Early adoption is permitted for all entities.

Table of Contents

INTRODUCTION

Overview of SASB Standards

The SASB Standards are a set of 77 industry-specific sustainability accounting standards ("SASB Standards" or "Industry Standards"), categorised pursuant to the Sustainable Industry Classification System® (SICS®).

SASB Standards include:

1. **Industry descriptions** – which are intended to help entities identify applicable industry guidance by describing the business models, associated activities and other common features that characterise participation in the industry.

2. **Disclosure topics** – which describe specific sustainability-related risks or opportunities associated with the activities conducted by entities within a particular industry.

3. **Metrics** – which accompany disclosure topics and are designed to, either individually or as part of a set, provide useful information regarding an entity's performance for a specific disclosure topic.

4. **Technical protocols** – which provide guidance on definitions, scope, implementation and presentation of associated metrics.

5. **Activity metrics** – which quantify the scale of specific activities or operations by an entity and are intended for use in conjunction with the metrics referred to in point 3 to normalise data and facilitate comparison.

Entities using the SASB Standards as part of their implementation of ISSB Standards should consider the relevant ISSB application guidance.

For entities using the SASB Standards independently from ISSB Standards, the *SASB Standards Application Guidance* establishes guidance applicable to the use of all Industry Standards and is considered part of the Standards. Unless otherwise specified in the technical protocols contained in the Industry Standards, the guidance in the SASB Standards Application Guidance applies to the definitions, scope, implementation, compilation and presentation of the metrics in the Industry Standards.

Historically, the *SASB Conceptual Framework* set out the basic concepts, principles, definitions and objectives that guided the SASB Standards Board in its approach to setting standards for sustainability accounting.

Use of the Standards

SASB Standards are intended to aid entities in disclosing information about sustainability-related risks and opportunities that could reasonably be expected to affect the entity's cash flows, its access to finance or cost of capital over the short, medium or long term. An entity determines which Industry Standard(s) and which disclosure topics are relevant to its business, and which associated metrics to report. In general, an entity should use the SASB Standard specific to its primary industry as identified in SICS® . However, companies with substantial business in multiple SICS® industries should refer to and consider the applicability of the disclosure topics and associated metrics in additional SASB Standards.

The disclosure topics and associated metrics contained in this Standard have been identified as those that are likely to be useful to investors. However, the responsibility for making materiality judgements and determinations rests with the reporting entity.

Industry Description

The Consumer Finance industry provides loans to consumers. Revolving credit loans through credit card products are the largest industry segment. Additional loan services may include automobile, micro-lending and student loans. Some industry entities also provide consumer-to-consumer money transfers, money orders, pre-paid debit cards and bill payment services. Industry performance is determined by consumer spending, rates of unemployment, per capita GDP, income and population growth. Trends towards consumer protection and transparency have aligned and will continue to align the interests of society with those of long-term investors.

Note: This Standard is limited to the abovementioned consumer finance services. A separate Standard addresses the sustainability-related risks and opportunities associated with mortgage finance activities.

SUSTAINABILITY DISCLOSURE TOPICS & METRICS

Table 1. Sustainability Disclosure Topics & Metrics

TOPIC	METRIC	CATEGORY	UNIT OF MEASURE	CODE
Customer Privacy	Number of account holders whose information is used for secondary purposes [1]	Quantitative	Number	FN-CF-220a.1
	Total amount of monetary losses as a result of legal proceedings associated with customer privacy [2]	Quantitative	Presentation currency	FN-CF-220a.2
Data Security	(1) Number of data breaches, (2) percentage that are personal data breaches, (3) number of account holders affected [3]	Quantitative	Number, Percentage (%)	FN-CF-230a.1
	Card-related fraud losses from (1) card-not-present fraud and (2) card-present and other fraud	Quantitative	Presentation currency	FN-CF-230a.2
	Description of approach to identifying and addressing data security risks	Discussion and Analysis	n/a	FN-CF-230a.3
Selling Practices	Percentage of total remuneration for covered employees that is variable and linked to the amount of products and services sold [4]	Quantitative	Percentage (%)	FN-CF-270a.1
	Approval rate for (1) credit and (2) pre-paid products for applicants [5]	Quantitative	Percentage (%)	FN-CF-270a.2
	(1) Average fees from add-on products, (2) average APR of credit products, (3) average age of credit products, (4) average number of credit accounts, and (5) average annual fees for pre-paid products	Quantitative	Presentation currency, Percentage (%), Months, Number	FN-CF-270a.3
	(1) Number of customer complaints filed, (2) percentage with monetary or non-monetary relief	Quantitative	Number, Percentage (%)	FN-CF-270a.4
	Total amount of monetary losses as a result of legal proceedings associated with selling and servicing of products [6]	Quantitative	Presentation currency	FN-CF-270a.5

[1] Note to **FN-CF-220a.1** – The entity shall describe its policies and procedures regarding how it discloses the use of customer data for third party use to customers, including the nature of its opt-in policy.

[2] Note to **FN-CF-220a.2** – The entity shall briefly describe the nature, context and any corrective actions taken because of monetary losses.

[3] Note to **FN-CF-230a.1** – The disclosure shall include a description of corrective actions implemented in response to data breaches.

[4] Note to **FN-CF-270a.1** – The entity shall describe remuneration policies for covered employees, including the link to products sold, the process for setting sale targets and benefits/penalties associated with meeting/missing the targets.

[5] Note to **FN-CF-270a.2** – The entity shall discuss its strategy for minimising credit deterioration of loans in its portfolio.

[6] Note to **FN-CF-270a.5** – The entity shall briefly describe the nature, context and any corrective actions taken because of monetary losses.

Table 2. Activity Metrics

ACTIVITY METRIC	CATEGORY	UNIT OF MEASURE	CODE
Number of unique consumers with an active (1) credit card account and (2) pre-paid debit card account[7]	Quantitative	Number	FN-CF-000.A
Number of (1) credit card accounts and (2) pre-paid debit card accounts	Quantitative	Number	FN-CF-000.B

[7] Note to **FN-CF-000.A** – For joint accounts, the entity shall include the number of customers whose personal information it collects.

Customer Privacy

Topic Summary

Entities in the Consumer Finance industry face risks and opportunities associated with using customer data for purposes other than those for which the data was originally collected (for example, targeted advertising or transfer to third parties). Ensuring the privacy of personal information and other account holders' data is an essential responsibility of the Consumer Finance industry. To assess performance on this issue, investors may benefit from entities' disclosure of the number of account holders whose information is used for secondary purposes, and their policies and procedures around using such information, including the nature of their opt-in policies. Investors may be encouraged and reassured by disclosures of information regarding an entity's data usage, as well as applicable jurisdictional legal or regulatory actions related to customer protection and privacy. Entities in the Consumer Finance industry that fail to manage performance in this area may be susceptible to decreased revenues resulting from lost consumer confidence and high employee turnover, as well as financial consequences arising from increased legal risks.

Metrics

FN-CF-220a.1. Number of account holders whose information is used for secondary purposes

1 The entity shall disclose the total number of unique account holders whose information is used for secondary purposes.

1.1 Account holder information is defined as data that pertains to an account holder's attributes or actions which may include account statements, transaction records, records of communications, content of communications, demographic data, behavioural data, location data and personal data.

1.1.1 Demographic data is defined as the information that identifies and distinguishes a given population. Examples of demographic data include gender, age, race/ethnicity, language, disabilities, mobility, home ownership and employment status.

1.1.2 Behavioural data is defined as information that tracks, measures and records individual behaviours, such as online browsing patterns, buying habits, brand preferences and product usage patterns.

1.1.3 Location data is defined as information that describes the physical location or movement patterns of an individual, such as Global Positioning System (GPS) coordinates or other related data that identifies and tracks an individual's physical location.

1.1.4 Personal data is defined as information that relates to an identified or identifiable living individual. Various pieces of information, which collected together can lead to the identification of a particular person, also constitute personal data.

1.1.5 The entity may define personal data based on applicable jurisdictional laws or regulations. In such cases, the entity shall disclose the applicable jurisdictional standard or definition used.

1.2 A secondary purpose is defined as the entity intentionally using data outside the primary purpose for which the data was collected. Examples of secondary purposes may include selling targeted advertisements and transferring data or information to a third party through sale, rental or sharing.

1.3 Customer accounts that the entity cannot verify as belonging to the same individual shall be disclosed separately.

2 The scope of the disclosure shall include the account holders whose information is used by the entity for secondary purposes, as well as the account holders whose information is provided to third parties, including those that directly or indirectly control, are controlled by, or are under common control with the entity, to use for secondary purposes.

Note to **FN-CF-220a.1**

1 The entity shall describe its policies and procedures regarding how it discloses to account holders the use of their information for secondary purposes, including the nature of its opt-in policy.

1.1 Opt-in is defined as explicit affirmative consent required to use or share content.

2 The scope of disclosure shall include:

2.1 how account holders provide consent for their information to be used for secondary purposes, such that the entity shall describe whether the consent is explicit, freely given, specific, informed or unambiguous; and

2.2 the extent to which the entity discloses to account holders the precise use of their information for secondary purposes, including whether and how the entity informs account holders about the specific data the entity intends to use for secondary purposes, the parties that have access to the data and how those parties may use the data.

3 The entity shall describe the regulatory environment related to account holder privacy in which it operates, which may include evolving regulations and risks related to regulatory compliance.

3.1 The description may include customer privacy policies and procedures adopted for regulatory compliance as well as policies and procedures adopted voluntarily as industry best practice.

FN-CF-220a.2. Total amount of monetary losses as a result of legal proceedings associated with customer privacy

1 The entity shall disclose the total amount of monetary losses incurred during the reporting period resulting from legal proceedings associated with incidents relating to customer privacy.

2 The legal proceedings shall include any adjudicative proceeding involving the entity, whether before a court, a regulator, an arbitrator or otherwise.

3 The losses shall include all monetary liabilities to the opposing party or to others (whether as the result of settlement, verdict after trial or otherwise), including fines and other monetary liabilities incurred during the reporting period as a result of civil actions (for example, civil judgements or settlements), regulatory proceedings (for example, penalties, disgorgement or restitution) and criminal actions (for example, criminal judgements, penalties or restitution) brought by any entity (for example, governmental, business or individual).

4 The scope of monetary losses shall exclude legal and other fees and expenses incurred by the entity in its defence.

5 The scope of the disclosure shall include legal proceedings associated with the enforcement of applicable jurisdictional laws or regulations.

Note to **FN-CF-220a.2**

1 The entity shall briefly describe the nature (for example, judgement or order issued after trial, settlement, guilty plea, deferred prosecution agreement or non-prosecution agreement) and context (for example, fraud, disclosure to clients or employee compensation) of all monetary losses resulting from legal proceedings.

2 The entity shall describe any corrective actions implemented in response to the legal proceedings. This may include specific changes in operations, management, processes, products, business partners, training or technology.

Data Security

Topic Summary

Entities in the Consumer Finance industry face risks and opportunities associated with customer data security management, in the context of external threats. Ensuring the security of customers' personal information is an essential responsibility of the Consumer Finance industry. To assess performance on this issue, analysts may benefit from disclosure regarding safeguarding customer data against emerging and continuously evolving cybersecurity threats and technologies, security breaches compromising customers' personal information, and credit and debit card fraud. Entities that fail to manage these threats effectively may be susceptible to reduced revenues resulting from decreased consumer confidence and high employee turnover. Furthermore, data breaches may expose entities to lengthy, costly litigation and potential monetary losses.

Metrics

FN-CF-230a.1. (1) Number of data breaches, (2) percentage that are personal data breaches, (3) number of account holders affected

1 The entity shall disclose (1) the total number of data breaches identified during the reporting period.

1.1 A data breach is defined as an unauthorised occurrence on, or conducted through, an entity's information systems that jeopardises the confidentiality, integrity or availability of an entity's information systems or any information contained therein.

1.1.1 Information systems are defined as information resources, owned or used by the entity, including physical or virtual infrastructure controlled by such information resources, or components thereof, organised for the collection, processing, maintenance, use, sharing, dissemination or disposition of an entity's information to maintain or support operations.

1.2 The scope of the disclosure excludes occurrences in which an entity has reasonable and supportable belief that the occurrence (i) does not pose a risk of damage to the entity's business performance or prospects and (ii) does not pose a risk of economic or social disadvantage to individuals.

2 The entity shall disclose (2) the percentage of data breaches that were personal data breaches.

2.1 A personal data breach is defined as a data breach resulting in the accidental or unauthorised destruction, loss, alteration, disclosure of, or access to, personal data transmitted, stored or otherwise processed.

2.2 Personal data is defined as any information that relates to an identified or identifiable living individual. Various pieces of information, which collected together can lead to the identification of a particular person, also constitute personal data.

2.2.1 The entity may define personal data based on applicable jurisdictional laws or regulations. In such cases, the entity shall disclose the applicable jurisdictional standard or definition used.

2.3 The scope of the disclosure shall include incidents during which encrypted data was acquired with an encryption key that also was acquired, as well as whether a reasonable belief exists that encrypted data could be converted readily to plaintext.

2.3.1 Encryption is defined as the process of transforming plaintext into ciphertext.

3 The entity shall disclose (3) the total number of unique account holders affected by personal data breaches.

3.1 Accounts that the entity cannot verify as belonging to the same account holder shall be disclosed separately.

4 The entity may delay disclosure if a law enforcement agency has determined that notification impedes a criminal investigation, and may be delayed until the law enforcement agency determines that such notification does not compromise the investigation.

Note to **FN-CF-230a.1**

1 The entity shall describe any corrective actions taken in response to data breaches, such as changes in operations, management, processes, products, business partners, training or technology.

2 All disclosure shall be sufficient such that it is specific to the risks the entity faces, but disclosure itself would not compromise the entity's ability to maintain data privacy and security.

3 The entity may disclose its policy for disclosing data breaches to affected account holders in a timely manner.

FN-CF-230a.2. Card-related fraud losses from (1) card-not-present fraud and (2) card-present and other fraud

1 The entity shall disclose the amount of card-related fraud losses incurred during the reporting period.

2 The entity shall disclose card-related fraud losses as (1) card-not-present (CNP) and (2) card-present and other fraud losses.

2.1 CNP fraud is characterised by the unauthorised use of a credit card number, the security code printed on the card, or the cardholder's address details for a transaction in a non-face-to-face setting with a merchant. CNP fraud may be conducted online, through mail, by phone or by other means.

2.2 Card-present fraud is characterised by the unauthorised use of a physical credit card for a transaction in a face-to-face setting with a merchant.

2.3 Other fraud includes identify theft and any fraudulent transaction that cannot be classified as CNP fraud.

3 The entity shall calculate card-related fraud losses as the total value of account holder transactions refunded to account holders (card holders) because of fraud.

4 The scope shall include losses from the unauthorised use of revolving consumer credit, debit and pre-paid debit cards, including instances of card-present fraud and instances of CNP fraud where the entity is liable for losses (for example, when a merchant uses a chargeback protection service).

5 The scope also shall include fraudulent transactions that the entity charged back to merchants (or their acquiring banks), including those related to CNP fraudulent activity.

FN-CF-230a.3. Description of approach to identifying and addressing data security risks

1 The entity shall describe its approach to identifying information system vulnerabilities that may pose a data security risk.

1.1 Vulnerability is defined as a weakness in an information system, implementation, system security procedure or internal control that could be exploited.

1.2 Data security risk is defined as the risk of any circumstance or event with the potential to affect organisational operations (including mission, functions, image or reputation), assets, individuals, other organisations or governments through an information system via unauthorised access, destruction, disclosure, modification of information or denial of service.

2 The entity shall describe its approach to managing identified data security risks and vulnerabilities, which may include operational procedures, management processes, structure of products, business partner selection, employee training and use of technology.

3 The entity shall discuss observed trends in type, frequency and origination of attacks on its data security and information systems.

4 The entity shall describe its policies and procedures for disclosing data breaches to its customers in a timely manner.

5 The entity's disclosure shall include a discussion of data and system security efforts that relate to new and emerging cyber threats and attack vectors facing the financial services industry.

5.1 Emerging cyber threats may include cyber threats arising from the use of near-field communication payment systems, mobile banking and web-based banking.

5.2 Attack vectors may include ransomware, loan stacking schemes, money mule schemes and remote access attacks.

6 The entity shall describe the data security regulatory environment in which it operates.

6.1 The discussion shall include data security policies and procedures the entity adopted for regulatory compliance or voluntarily as an industry best practice.

7 The entity shall describe the degree to which its approach aligns with an external standard or framework or applicable jurisdictional legal or regulatory framework for managing data security, such as:

7.1 the ISO/IEC 2700 series;

7.2 the National Institute of Standards and Technology (NIST), *Framework for Improving Critical Infrastructure Cybersecurity*, 2018;

7.3 the New York State Department of Financial Services 23 NYCRR 500, *Cybersecurity Requirements for Financial Services Companies*; and

7.4 the Office of the Comptroller of the Currency (OCC) Bulletin 2013-29, *Third-Party Relationships: Risk Management Guidance*, 2013.

8 All disclosure shall be sufficient such that it is specific to the risks the entity faces, but disclosure itself would not compromise the entity's ability to maintain data privacy and security.

Selling Practices

Topic Summary

Selling practices encompasses performance in three important areas that can affect an entity's operations and financial condition. First, entity compensation and incentive policies may unintentionally encourage the selling of products and services that are not in the clients' best interest. Secondly, an entity may be perceived as using deceptive practices from a failure to provide transparent information to customers about primary and add-on products. And finally, depending on the characteristics of products offered, poor performance on the first two elements could result in customers holding portfolios containing high concentrations of risk. Entities in the Consumer Finance industry may face increased scrutiny as regulators encourage improved transparency and enhanced disclosure. The disclosure of important lending portfolio characteristics—including average fees from add-on products, average age of credit products, average annual percentage rate (APR) of credit products, average number of credit accounts and average annual fees for pre-paid transaction products—may permit shareholders to determine which entities can best protect long-term value, rather than relying on short-term revenue generation practices. Providing consumer finance products focused on the customers' best interest may build trust with new and existing customers, expand market share, and ensure sustainable revenue growth.

Metrics

FN-CF-270a.1. Percentage of total remuneration for covered employees that is variable and linked to the amount of products and services sold

1 The entity shall disclose the percentage of total variable remuneration accrued for covered employees during the reporting period.

1.1 Variable remuneration is defined as all remuneration that is not fixed.

1.2 Remuneration is fixed if all the conditions for its award and its amount:

1.2.1 are based on predetermined criteria and are non-discretionary, reflecting the level of professional experience and seniority of staff;

1.2.2 are transparent with respect to the individual amount awarded to the individual staff member;

1.2.3 are permanent, maintained over a period tied to the specific role and organisational responsibilities;

1.2.4 are non-revocable, meaning that the permanent amount is only changed via collective bargaining or following renegotiation in line with national criteria on wage-setting;

1.2.5 cannot be reduced, suspended or cancelled by the institution;

1.2.6 do not provide incentives for risk assumption; and

1.2.7 do not vary with performance.

1.3 Covered employees are defined as individuals employed by the entity that are engaged in selling products or services directly to customers or potential customers, and include those categorised by the entity into categories equivalent to (a) sales workers, and (b) first- and mid-level officers and managers – sales managers, in accordance with, and further facilitated by, any applicable jurisdictional laws, regulations, guidance or generally accepted definitions.

2 The percentage shall be calculated as the aggregate amount of variable remuneration linked to covered employee products and services sales divided by the aggregate amount of total covered employee remuneration, for the reporting period.

Note to **FN-CF-270a.1**

1 The disclosure shall include a discussion regarding how covered employee remuneration relates to the terms and conditions of the products and services, such as interest rates, up-front points or fees.

2 The entity shall discuss how it set performance targets and what monetary and non-monetary benefits or penalties were employed for meeting or missing these targets.

3 The discussion shall include:

3.1 the employee remuneration regulatory environment in which the entity operates and whether it must use specific remuneration policies; the entity shall discuss whether its remuneration policies were adopted in response to regulatory requirements or voluntarily as industry best practice;

3.2 the performance objectives for the institution, business areas and staff;

3.3 the methods for the measurement of performance, including performance criteria; and

3.4 the structure of variable remuneration, including (if applicable) the instruments in which parts of the variable remuneration were awarded.

FN-CF-270a.2. Approval rate for (1) credit and (2) pre-paid products for applicants

1 The entity shall disclose the approval rate for its (1) credit and (2) pre-paid products for all applicants in the reporting period.

1.1 Pre-paid products include pre-paid accounts and cards, excluding checking accounts, share draft accounts or negotiable order of withdrawal (NOW) accounts, or similar accounts.

2 The entity shall calculate the approval rate as the number of applications approved from applicants divided by the total number of applications received from applicants.

3 The scope of the disclosure includes applications the entity approved or denied during the reporting period, regardless of when the application was received.

Note to **FN-CF-270a.2**

1 The entity shall discuss its short- and long-term credit and pre-paid product portfolio performance management strategy.

1.1 The discussion shall include the entity's strategy for minimising credit deterioration of loans in its portfolio.

FN-CF-270a.3. (1) Average fees from add-on products, (2) average APR of credit products, (3) average age of credit products, (4) average number of credit accounts, and (5) average annual fees for pre-paid products

1 The entity shall disclose (1) the average fees from add-on products for all customers.

1.1 Add-on products may include debt protection, identity theft protection, credit score tracking and other products supplementary to the credit provided by the card itself and offered at additional cost to consumers.

1.2 The entity shall calculate the average fees from add-on products as the total amount of revenue generated from add-on products from customers divided by the total number of the entity's customers, for the reporting period.

2 The entity shall disclose (2) the average annual percentage rate (APR) of all credit products.

2.1 The entity shall calculate the average APR for all credit products' assessed interest during the reporting period as the annualised ratio of total finance charges to the total average daily balances, against which the finance charges were assessed (excluding accounts for which no finance charges were assessed).

2.1.1 Definitions of finance charge and detailed calculation of APR may be defined using applicable jurisdictional laws or regulations.

2.1.2 A finance charge is defined as all charges payable directly or indirectly to the consumer and imposed directly or indirectly by the creditor as an incident to, or a condition of the extension of credit.

3 The entity shall disclose (3) the average age of credit products in months for all customers.

3.1 The entity shall calculate the average age of credit products (in months) from the date that each active account was opened until the close of the reporting period.

4 The entity shall disclose (4) the average number of credit accounts for all customers.

4.1 The entity shall calculate the average number of credit accounts per customer as the number of credit accounts held by customers divided by the total number of customers.

5 The entity shall disclose (5) the average annual fees for pre-paid products for all customers.

5.1 Pre-paid products include pre-paid accounts and cards, excluding checking accounts, share draft accounts or negotiable order of withdrawal (NOW) accounts, or similar accounts.

5.2 The entity shall calculate the average annual fees for pre-paid products as the total amount of revenue generated from pre-paid products from customers divided by the total number of the entity's customers.

6 The entity may disaggregate its disclosure by customer characteristics such as creditworthiness.

FN-CF-270a.4. (1) Number of customer complaints filed, (2) percentage with monetary or non-monetary relief

1 The entity shall disclose (1) the total number of customer complaints filed with the applicable jurisdictional legal or regulatory agencies or other organisations during the reporting period for which the entity was a defendant in the complaint.

1.1 Legal or regulatory agency or other organisation refers to any financial regulator or other organisation, such as a financial ombudsman, that is authorised to handle complaints regarding financial products and services offered to consumers in the applicable jurisdiction.

1.2 The entity shall disclose the name and a description of the agencies or other organisations used in preparing its disclosure.

2 The entity shall disclose (2) the percentage of complaints filed with the applicable jurisdictional legal or regulatory agency or other organisation that resulted in monetary or nonmonetary relief.

2.1 Monetary relief and non-monetary relief are defined according to the applicable jurisdictional legal or regulatory agency or another organisation.

2.2 The disclosure scope includes complaints filed during the reporting period.

3 The disclosure scope shall include the complaints filed regarding these product categories:

3.1 credit cards or pre-paid cards;

3.2 student loans;

3.3 vehicle loans or leases;

3.4 payday loans, title loans and other personal loans; and

3.5 money transfers, virtual currencies, or other money services.

4 The disclosure scope shall include these issues:

4.1 selling practices;

4.2 transparent information;

4.3 advertising and marketing;

4.4 fees and interest;

4.5 add-on products;

4.6 account servicing;

4.7 application process; and

4.8 closing the account.

5 The entity may provide a breakdown by type of product or issue.

FN-CF-270a.5. Total amount of monetary losses as a result of legal proceedings associated with selling and servicing of products

1 The entity shall disclose the total amount of monetary losses incurred during the reporting period resulting from legal proceedings associated with selling and servicing of products.

2 The legal proceedings shall include any adjudicative proceeding involving the entity, whether before a court, a regulator, an arbitrator or otherwise.

3 The losses shall include all monetary liabilities to the opposing party or to others (whether as the result of settlement, verdict after trial or otherwise), including fines and other monetary liabilities incurred during the reporting period as a result of civil actions (for example, civil judgements or settlements), regulatory proceedings (for example, penalties, disgorgement or restitution) and criminal actions (for example, criminal judgements, penalties or restitution) brought by any entity (for example, governmental, business or individual).

4 The scope of monetary losses shall exclude legal and other fees and expenses incurred by the entity in its defence.

5 The scope of the disclosure shall include legal proceedings associated with the enforcement of applicable jurisdictional laws or regulations.

Note to **FN-CF-270a.5**

1 The entity shall briefly describe the nature (for example, judgement or order issued after trial, settlement, guilty plea, deferred prosecution agreement or non-prosecution agreement) and context (for example, fraud, disclosure to clients or employee compensation) of all monetary losses resulting from legal proceedings.

2 The entity shall describe any corrective actions implemented in response to the legal proceedings. This may include specific changes in operations, management, processes, products, business partners, training or technology.

SASB STANDARDS

Now part of IFRS Foundation