9 September 2024

Financial Supervisory Commission
18F., No. 7, Sec. 2, Xianmin Blvd.
Banqiao District
New Taipei City 220232

To the Financial Supervisory Commission

Proposed Amendments to the Regulations Governing the Security Maintenance of Personal Data Files for Non-government Agencies Designated by the Financial Supervisory Commission

On behalf of its members, the Asia Securities Industry & Financial Markets Association ("**ASIFMA**")[1] ("**we**," "**our**" or "**us**") are pleased to submit this letter to the Financial Supervisory Commission ("**FSC**"). We seek to convey the industry's views on the proposed amendments ("**Draft Amendments**") to the Regulations Governing the Security Maintenance of Personal Data Files for Non-government Agencies Designated by the Financial Supervisory Commission ("**Data Security Regulations**") and offer constructive ideas on how the Draft Amendments can be refined to encourage foreign investment into the Republic of China ("**ROC**" or "**Taiwan**"), enhance risk management and facilitate compliance by financial institutions ("**FIs**") with robust standards and obligations aligned with those of other jurisdictions that are considered integral to world markets.

Summary of key concerns

1. Removal of materiality threshold for data breach notification requirements

The Draft Amendments remove the threshold of materiality for data breach notifications to the FSC under Paragraph 2, Article 6 of the Data Security Regulations and deletes the definition of "significant data breach" under Paragraph 3, Article 6 of the Data Security Regulations.

Removing the materiality threshold will result in a burdensome reporting process for both FIs and the FSC, even for incidents involving only a single individual. Frequent reporting without considering materiality may also dilute the focus and attention needed for incidents that pose a genuine risk of harm.

We urge the FSC to maintain the materiality qualifier and/or the criterion of actual harm by limiting the data breach notification requirements to incidents that are likely to jeopardize FIs' normal

[1] ASIFMA is an independent, regional trade association with over 160 member firms comprising a diverse range of leading FIs from both the buy and sell side, including banks, asset managers, law firms and market infrastructure service providers. Together, we harness the shared interests of the financial industry to promote the development of liquid, deep and broad capital markets in Asia. ASIFMA advocates stable, innovative, competitive and efficient Asian capital markets that are necessary to support the region's economic growth. We drive consensus, advocate solutions and effect change around key issues through the collective strength and clarity of one industry voice. Our many initiatives include consultations with regulators and exchanges, development of uniform industry standards, advocacy for enhanced markets through policy papers, and lowering the cost of doing business in the region. Through the GFMA alliance with SIFMA in the United States and AFME in Europe, ASIFMA also provides insights on global best practices and standards to benefit the region.

operations or the interests of a significant number of data subjects.

2. Shortening notification timeframe from 72 hours to 48 hours

Paragraph 2, Article 6 of the Draft Amendments shortens the notification timeframe for FIs to report data breaches from 72 hours to 48 hours.

We understand that Taiwan's Personal Data Protection Act ("**PDPA**") currently does not mandate the reporting of data breaches to regulators. Nonetheless, reporting a data breach to competent authorities may be required under those regulations established by certain central competent authorities for the specific industry sectors under their charge. In the financial sector, FIs are already subject to stringent supervision by the FSC and other competent authorities, as well as various and stricter reporting requirements under different laws and regulations, including those mandating shorter timeframes for reporting cybersecurity incidents.

Furthermore, in practical operations, shortening the notification timeframe from 72 hours to 48 hours would pose significant challenges, particularly when this period overlaps with weekends or holidays, as it would significantly reduce the time available for FIs to identify, contain, assess, and report data breaches. Moreover, it is important to consider international benchmarks in data privacy regulations. For instance, the EU General Data Protection Regulation (GDPR) mandates a 72-hour notification period for data breaches, which implies that the 72-hour timeframe is regarded as a reasonable and practically feasible standard, allowing organizations sufficient time to accurately identify data breaches, assess and contain their impact, and prepare a comprehensive notification. Adopting a similar timeframe that aligns with global benchmarks and best practices will ensure that organizations are not unduly burdened, thereby maintaining a balance between prompt reporting and practical feasibility.

In light of these considerations, we urge the FSC to evaluate the extensive reporting requirements imposed on FIs and international regulatory standards thoroughly and to maintain the existing 72-hour notification timeframe.

3. Introduction of one-hour notification requirements for "significant and high-profile data breach"

The proviso of Paragraph 2, Article 6 of the Draft Amendments introduces new notification requirements for "significant and high-profile data breaches," requiring FIs to notify the FSC of a significant and high-profile data breach within one hour upon becoming aware thereof. Paragraph 4, Article 6 of the Draft Amendments further defines "significant and high-profile data breach" as follows:

(1) A data breach attracting a lot of attention from the Executive Yuan, Legislative Yuan, or Control Yuan; or

(2) A data breach notably covered by media, e.g., nationwide coverage in the print media or focused discussions in the electronic media.

However, it is obvious that the definition of "significant and high-profile data breach" only provides criteria for determining whether a data breach is high-profile and does not include any materiality threshold, which compels FIs to predict which data breaches will attract media or government attention and requires them to evaluate whether an incident is reportable based on media publication rather than their risk assessments. Furthermore, the exact nature of "electronic media"

cannot be definitively identified. It is unclear whether it refers to electronic editions of traditional print media or includes social media websites. Given the time constraint, this could practically result in all incidents being reported to the FSC as long as FIs become aware of any media exposure (even if there is only one individual who asserted to have been affected on a social media website or there is no indication that the incident may result in any risk to the affected individuals).

In addition, considering the internal operational process, it is practically difficult and not feasible for FIs to satisfy the one-hour notification timeframe upon becoming aware of a data breach. FIs typically have multi-layered systems that require investigations to confirm the breach and assess its scope and impact. This process involves coordination among various departments such as IT, legal, compliance, and risk management, which can be time-consuming. Therefore, a more realistic and reasonable timeframe would allow FIs to conduct a preliminary assessment and provide accurate and useful information to the FSC.

To address this issue practically, we recommend that the FSC (i) extend the one-hour notification timeframe to a more reasonable period (e.g., 24 hours upon becoming aware of a significant and high-profile data breach), (ii) include the materiality threshold in the definition of "significant and high-profile data breach," and (iii) offer additional clarification and comprehensive guidelines on the criteria and procedures for FIs to identify and report significant and high-profile data breaches.

Next steps

As we understand the importance of such regulation for Taiwan's business and economic environment, we would be pleased to engage in further discussions with the FSC. ASIFMA and our members are ready to provide further details and to engage in constructive dialogue on the Draft Amendments.

Should you have any questions about this letter or would like to obtain further industry input, please contact Diana Parusheva, Managing Director at ASIFMA, Head of Public Policy and Sustainable Finance at dparusheva@asifma.org.

This submission was prepared based on feedback from the wider ASIFMA membership.

Yours faithfully

Diana Parusheva - Lowery

Managing Director

Head of Public Policy and Sustainable Finance

Asia Securities Industry & Financial Markets Association

M: +852 9822 2340

DParusheva@asifma.org