Administrative Measure Publication Notice

This notice is being published by the Financial Intelligence Analysis Unit (FIAU) in terms of Article 13C of the Prevention of Money Laundering Act ("PMLA") and in accordance with the policies and procedures on the publication of AML/CFT measures established by the Board of Governors of the FIAU. This notice provides select information from the FIAU's decision imposing the respective administrative measures, and is not a reproduction of the actual decision.

DATE OF IMPOSITION OF THE ADMINISTRATIVE MEASURE:
24 November 2020

SUBJECT PERSON:
Insignia Cards Limited

RELEVANT FINANCIAL BUSINESS CARRIED OUT:
Financial Institution

SUPERVISORY ACTION:
On-site compliance review carried out in 2019

DETAILS OF THE ADMINISTRATIVE MEASURES IMPOSED:
Administrative Penalty of €373,670, Reprimand and a Follow-up Directive in terms of Regulation 21 of the Prevention of Money Laundering and Funding of Terrorism Regulations ("PMLFTR").

LEGAL PROVISION BREACHED:

- Regulation 5(1) and 5(5)(a) of the PMLFTR and Section 3.3 of the Implementing Procedures ("IPs") Part 1;
- Regulation 5 of the PMLFTR and Section 3.5 of the IPs;
- Regulation 7(1)(a) and 7(1)(b) of the PMLFTR;
- Regulation 7(1)(c) of the PMLFTR and Section 4.4 of the IPs;
- Regulation 11 of the PMLFTR;
- Regulation 12(2) of the PMLFTR;
- Regulation 7(1)(d) of the PMLFTR and Section 4.5.3 of the IPs;
- Regulation 7(2)(a) of the PMLFTR and Section 4.5.2 of the IPs; and
- Regulation 15 of the PMLFTR and Section 5.1, 5.4, 5.5 and 5.7 of the IPs.

REASONS LEADING TO THE IMPOSITION OF THE ADMINISTRATIVE MEASURES:

Regulation 5(1) and 5(5)(a) of the PMLFTR and Section 3.3 of the IPs Part 1

Several deficiencies were identified in relation to the Business Risk Assessment ("BRA") in place during the compliance examination. Some of such deficiencies are being relayed hereunder:

- The BRA held insufficient information to understand the threat emanating from the vulnerabilities identified by Insignia Cards Limited (the "Company"), in particular those presenting a high or extreme inherent risk;
- The controls listed within the Company's BRA lacked the required detail and were in some instances described in an abbreviated manner;
- Lacking information was found to explain how the Company had determined that any of the mitigating measures it has adopted are suitable or adequate in relation to the identified vulnerabilities.

Hence, the FIAU's Compliance Monitoring Committee (the "Committee") determined that the Company is in breach of Regulation 5(1) and 5(5)(a) of the PMLFTR and Section 3.3 of the IPs.

Regulation 5 of the PMLFTR and Section 3.5 of the IPs

The Compliance examination identified serious concerns pertaining to the Company's Customer Risk Assessment ("CRA") methodology and additionally its ineffective implementation. The Committee's concerns are being relayed hereunder:

- In relation to the risks emanating from non-reputable jurisdictions, the Company's CRA methodology allowed for customers to be rated a lower risk rating rather than that required in terms of Regulation 11(1)(c) of the PMLFTR and Section 4.9.1 of the IPs, being high ML/FT risk;
- The risk-scoring grid used by the Company to risk-rate its customers works to minimise the risk rating of customers rather than identifying the true risks. This since, although the Company's CRA methodology classifies most of the customers as presenting a medium inherent risk at on-boarding, a more comprehensive methodology would have portrayed a more accurate assessment of the risk presented by the customer, leading to the identification of higher risk exposures;
- The compliance examination identified that for six (6) files reviewed, CRA was not carried out at all. Furthermore, CRA was not performed until September 2019 for clients introduced by one of the Company's reliance partners; hence the Company was on-boarding customers from such partner without even understanding the risks involved through such relationships;
- Moreover, for twenty-one (21) files reviewed, CRA was carried out late, on average over two (2) years after the customer's account had been activated.

In view of the above, the Committee determined that the findings identified constitute systemic breaches of Regulation 5 of the PMLFTR and Section 3.5 of the IPs.

Regulation 7(1)(a) and 7(1)(b) of the PMLFTR

The Committee noted overall good processes and that the Company does have necessary measures to ensure it obtains identification information and verification documentation about its customers. However, during the on-site compliance review, officials noted that in nine (9) files, the Company still failed to either verify or otherwise completely verify the identity of the customers and/or supplementary card holders. Furthermore, certification performed by the Company's employees were in some cases not dated. Hence the Committee determined that the Company is in breach of its obligation in terms of Regulation 7(1)(a) and 7(1)(b) of the PMLFTR.

Regulation 7(1)(c) of the PMLFTR and Section 4.4 of the IPs

The Committee determined that during the compliance examination the Company failed to collect, in three (3) of the files reviewed, adequate information on the purpose and intended nature of the business relationship and that required to establish the customer business and risk profile.

- For example, in one file pertaining to a private holding company incorporated in Gibraltar and introduced by one of the Company's reliance partners, the Company failed to obtain any information on the source of wealth and source of funds of the customer, for which the Company stated, this in view of the reliance agreement in place. However, the Committee emphasises that as per Section 4.10.4 of the IPs, regardless of the fact that the subject person is relying on another entity for the fulfilment of CDD requirements, the subject person must still obtain the information concerning the customer's identity, the identity of the beneficial owner(s) (where applicable), the information on the purpose and intended nature of the business relationship and the customer's business and risk profile. All this information must be obtained by the subject person before carrying out an occasional transaction or entering into a business relationship.

In view of the above, such findings have been deemed as breaches to Regulation 7(1)(c) of the PMLFTR and Section 4.4 of the IPs.

Regulation 11 of the PMLFTR

The compliance examination identified that although the Company's AML/CFT Policy correctly details situations for which EDD is required, such policy was missing a crucial element; this being to describe the additional measures required to be undertaken in addition to the standard due diligence procedures. Therefore, although the policy refers to the need to carry out EDD, the measures that need to be applied are not prescribed which leaves room for subjectivity in its application. Careful consideration of what and how EDD measures should be carried out is important in general for all subject persons, but particularly crucial for the Company, having itself marked its own business as posing high ML/FT risk exposure.

The Committee's concerns are further corroborated as evidence of this shortcoming was further highlighted when the officials undertaking the Compliance examination reviewed actual customer files which exposed the Company to higher risks. This due to the fact that the Company failed to carry out the necessary EDD measures in four (4) files reviewed albeit classifying the customer as high risk.

- For example, one file pertaining to a natural person was risk rated by the Company as high-risk due to his politically exposed status and adverse media links pertaining to ties with the Russian mafia. However, as an EDD measure to potentially mitigate the serious nature of the allegations and ML/FT exposure emanating from such customer, the Company was satisfied with only obtaining, through an independent source, the Company's internal source of wealth declaration form. However, such source of wealth declaration form only corroborated the information of the customer's estimated earnings, his estimated assets, source of wealth stated as originated from employment and details pertaining to such individual's employment and as being an executive director of an entity, being the co-founder of another entity and that over the years had different entertainment businesses.

  However, the Committee determined that the source of wealth declaration, on its own, does not provide sufficient comfort pertaining to the legitimate origin of the source of wealth and source of funds which are to pass through the Company, this in particular in view of the heightened risk emanating from the customer's political status. Hence, at a minimum the Company should have in addition to the source of wealth declaration, requested the customer to provide documentary evidence to substantiate the declared income and the source that generated the customer's funds and wealth. By way of example obtaining payslips/ employment contracts if funds were the result of employment, evidence of dividend distribution if the customer had interest in companies, or evidence of interest paid in cases of contracts requiring the payment of interest.

The Company's high risk business model compounds even further the Committee's concerns on the Company's inadequate regard to ensuring effective measures for dealing with higher risk customers. In view of the above considerations, the Committee determined that the Company is in breach of Regulation 11 of the PMLFTR.

Regulation 12(2) of the PMLFTR

The Compliance examination identified that the Company has placed reliance on the CDD measures carried out by a number of credit institutions. Two (2) of such reliance relationships were attested during the compliance examination to ensure these entities met the requirements set out in Regulation 12(2) of the PMLFTR. However a number of deficiencies have been identified, some of which are being relayed hereunder:

- For both reliance relationships reviewed, despite the Company's statement that an assessment on such entities was carried out, the Company acknowledged that the assessment was not properly documented;
- For one of the reliance relationships attested, the Committee noted that since the commencement of the reliance arrangement in June 2016 up to the date of such confirmation provided in May 2020, hence for approximately four (4) years, the Company was relying on another party without being sure that such party was applying adequate CDD measures;
- Furthermore, the Committee determined that the Company also failed to assess possible risks that could emanate from the reliance relationship with both reliance partners.

The Committee considered that the obligation to carry out an assessment on the subject persons or third parties for which reliance is placed on, was enforced through the revised version of the IPs, last amended July 2019. This being just two (2) months prior the start of the compliance examination

undertaken on the Company. However, the Committee also considered that the Company was heavily dependent on the reliance agreements in the carrying out of customer due diligence measures and that therefore, the Company was expected to ensure that such obligation was immediately adhered to. In view of the above considerations, the Committee decided that the Company was during the time of the compliance examination in breach of Regulation 12(2) of the PMLFTR.

Regulation 7(1)(d) of the PMLFTR and Section 4.5.3 of the IPs

During the compliance examination, it was identified that file reviews were carried out only because there was a trigger that led the Company to review the details it has on the customer. Therefore, in all other instances where no particular trigger event occurred, the Company proceeded without any form of monitoring being implemented. The Company therefore failed to comprehensively implement measures to ensure that documents, data and information are kept up to date.

In view of the above, for twelve (12) of the files reviewed and which were actively transacting, the Company failed to undertake a periodic ongoing review, despite such review being due as per the Company's own AML procedures. Hence, the Committee determined that the Company is deemed to be in breach of Regulation 7(1)(d) of the PMLFTR and section 4.5.3 of the IPs.

Regulation 7(2)(a) of the PMLFTR and Section 4.5.2 of the IPs

The compliance examination identified serious shortcomings pertaining to the Company's inadequate scrutiny of customer transactions throughout the course of the business relationship. Furthermore, the Company failed to ensure that the transactions undertaken are consistent with the subject person's knowledge of the customer and of his business and risk profile. Some of the shortcomings identified are being relayed hereunder:

- The Company confirmed that it first implemented transaction monitoring on card spending in 2017. Furthermore, the Company stated that the transaction monitoring process in place prior to 2017 was to review unusual transactions in accordance with the Company's 'Transaction Matrix'. However, the Committee cannot ascertain the date this matrix started to be implemented by the Company, as it was not documented in the Company's ongoing monitoring procedures, this as was also advised by the Company during the examination. Hence, the Company, had since it started providing "relevant financial business" up to the implementation of measures for monitoring transactions in 2017 (approximately for 5 years), failed to adequately conduct transaction monitoring/ scrutiny that takes into account ML risks and typologies for customer spending through cards offered by the Company.

- The Committee determined that the transaction monitoring procedures in place by the Company for the period 2017 – June 2019 failed to define any rules to flag suspicious transaction activity. This since, the procedure document mainly provides instructions as to how the officer compiling the report is to navigate through the use of the Excel document and states that any suspicious behaviour is to be raised to the MLRO. However, what did or did not constitute suspicious activity/behaviour was left to the subjective judgement of the tasked employee. Moreover, there were no parameters that guided the basis for transactional activity to be discounted as not requiring further investigation or otherwise. The Committee further considered that, when questioned by FIAU officials, the Company officials replied that

transaction monitoring checks and compliance checks started from 1 June 2019, hence, for transactions undertaken prior to June 2019 no additional explanations and supporting documentation were able to be provided.

- Following the implementation of a partially automated transaction monitoring system, the Company's procedures updated post June 2019 explained the set of five (5) rules on which alerts are generated and flagged for review. While the Committee acknowledged that the rules are indeed adequate, additional rules are required, as the Company still lacked in assessing essential aspects in line with its transaction monitoring obligations. The rules employed by the Company's transaction monitoring system generates alerts on a one-size-fits-all basis. Therefore, the Company is unable to adequately identify behaviour or transactions that diverge from the usual pattern of transactions of its customers, nor is the Company able to ascertain that the transactions undertaken fit within the customer's profile or are otherwise not in line with what is normally expected from the said customer. By way of example:
    - In one file the Company had recorded customer's source of wealth to have accrued exclusively from his annual income of GBP 150,000, such funds derived from the customer's full-time employment. However, during the first months of 2019, such customer made payments amounting to approximately EUR 1.2 million. This including approximately EUR 208,500 to a car dealership in Monaco.

Furthermore, most of the settlement payments tested during the compliance examination were transferred into the Company's bank accounts from the Company's interrelated company incorporated in Hong Kong. The Company presented to FIAU officials a one-page procedure document (dated March 2019) pertaining to the process undertaken when dealing with such payments. Within such procedure, reference is made to the Company's controls in place to mitigate the exposure from such incoming payments. One of the controls noted relates to the Company's finance team requesting payment allocation details, as well as a bank credit advice statement bearing the name of the customer and specifying the payment amount, with such communication also being received by the Company's compliance team. However, a number of shortcomings pertaining to such process along with its ineffective implementation are being relayed hereunder:

- The Committee expressed its concerns that prior to March 2019, the Company failed to have any processes and procedures to identify the source and origin of funds of the repayments carried out by the customers through the Hong Kong entity. Furthermore, the controls as outlined within the Company's procedure dated 6 March 2019 were still inadequate to provide the required comfort to sufficiently establish, on a risk sensitive basis, the source of funds for incoming settlement payments made through the interrelated company in Hong Kong. This due to the fact that simply obtaining a credit advice, would not provide the required comfort to confirm that the incoming funds originated from non-illicit activities.
- In attempting to verify the controls in place, the Company was unable, in some instances, to provide the credit advice stated to have been collected. Therefore, the Company was not adequately implementing its own policies and procedures.

In view of the above, the Committee determined that the Company has breached its AML/CFT obligation as per Regulation 7(1)(d), 7(2)(a) of the PMLFTR and Section 4.5.2 of the IPs.

Regulation 15 of the PMLFTR and Section 5.1, 5.4, 5.5 and 5.7 of the IPs

In one (1) file, the Company did not raise an internal investigation to understand whether a Suspicious Transaction Report ("STR") should have been submitted to the FIAU. While in another two (2) instances, the Company's MLRO failed to submit a Suspicious Transaction Report to the FIAU concerning the activities of its customers. One example of such case is being explained hereunder:

- For one file, pertaining to a natural person, it was observed that the Company at on-boarding, in April 2018, risk rated the customer as 'medium', which subsequently had the assigned risk rating increased to 'high', in January 2019. The risk increase of this customer stemmed from serious red-flags pertaining to the said customer and his wife (who was also a customer of the Company), as in 2012 they were convicted of £2m fraud, as they were found to be listing thousands of pounds' worth of illicit tickets. It was noted that the customer carried out transactions via the cards provided by the Company to merchants of theatrical ticket agencies and that the customer sent payments to online ticket platforms. These same platforms were connected to the fraudulent activities the customer was accused of in 2012. Despite having sufficient information to suspect that its customer was connected to money laundering, no STR was submitted to the FIAU.

Hence, the Committee determined that the findings identified constitute as a breach of Regulation 15 of the PMLFTR and Section 5.1, 5.4, 5.5 and 5.7 of the IPs.

ADMINISTRATIVE MEASURES TAKEN BY THE FIAU'S COMPLIANCE MONITORING COMMITTEE:

After taking into consideration the abovementioned findings, the Committee remains concerned about the degree and extent of the Company's lack of adherence to its AML/CFT obligations. The majority of the failures have been considered by the Committee as very serious, which seriousness is compounded when taking into consideration the high risk business model of the Company's operations. The seriousness of these findings has led the Committee to impose an administrative penalty of three hundred and seventy-three thousand six hundred and seventy euro (€373, 670) with regards to the breaches identified in relation to:

- Regulation 5(1) and 5(5)(a) of the PMLFTR and Section 3.3 of the Implementing Procedures ("IPs") Part 1;
- Regulation 5 of the PMLFTR and Section 3.5 of the IPs;
- Regulation 7(1)(c) of the PMLFTR and Section 4.4 of the IPs;
- Regulation 11 of the PMLFTR;
- Regulation 7(2)(a) of the PMLFTR and Section 4.5.2 of the IPs; and
- Regulation 15 of the PMLFTR and Section 5.1, 5.4, 5.5 and 5.7 of the IPs.

In addition to the above, the Committee imposed a Reprimand in relation to the minor breaches identified for the Company's failures in terms of Regulation 7(1)(a) and 7(1)(b) of the PMLFTR.

The Committee positively acknowledged the actions already taken by the Company and the actions planned to be taken by it in order to remediate the failures identified during the compliance review. Said enhancements include and are not limited to: updates to the Company's CRA methodology; AML/CFT reviews being undertaken on its existing reliance partners; and also enhancements to its transaction monitoring measures. The Committee expects the Company to ensure that the remediation, both that has already been undertaken and that still planned to be undertaken, is effectively implemented. Hence, to ensure that the Company's remediation is adhered to, the

Committee also served the Company with a Follow-Up Directive. Through the Directive, the FIAU is requesting the Company to make available a detailed action plan pertaining to all the breaches identified following the compliance examination, along with any other relevant enhancements the Company has implemented/ plans to implement. The action plan is to include clear reference as to when the actions are to be completed, where applicable to provide supporting evidence and is to explain:

- How the Company shall take into consideration existing experience in determining the threat it is exposed to and in assessing whether the mitigating measures it has adopted/ will adopt within its Business Risk Assessment are suitable or adequate in relation to the identified vulnerabilities;
- The remedial action undertaken pertaining to the Company's Customer Risk Assessment Methodology. This along with the Company's plan to ensure that its active customers CRAs are updated and in line with the applicable AML/CFT obligations;
- How the Company plans to ensure that, for its active customers, it holds adequate information pertaining to the purpose and intended nature of the business relationship and that it acquires the required information/details/evidence to build a comprehensive risk profile in line with the applicable AML/CFT obligations;
- The EDD measures undertaken and why such measures are deemed as adequate;
- The remediation applied by each Reliance Partner relationship so as to ensure they are in line with the applicable AML/CFT obligations;
- The remediation already initiated by the Company in ensuring that documents, data and information are up to date;
- The revised transaction monitoring policies and procedures and explain how the Company is to ensure that the transaction monitoring obligations are adequately adhered to. Furthermore, how the Company shall ensure it is in a position to generate internal alerts for review to determine whether STRs should be reported to the FIAU;
- The remediation undertaken to revise its policies and procedures pertaining to transactions happening through other parties, this in particular to explain how the Company intends to adequately scrutinise such payments and ensure their legitimacy.

In determining the appropriate administrative measures to impose, the Committee took into consideration the representations submitted by the Company, together with the remedial actions that the Company had already started to implement. The nature and size of the Company's operations and the overall impact that the AML/CFT shortcomings of the Company have caused or could have caused both to its own operations and also to the local jurisdiction were also taken into account by the Committee. The seriousness of the breaches identified together with their occurrence were also considered by the Committee in determining the administrative measures imposed.

Finally, the Company has also been duly informed that in the eventuality that it fails to provide the above mentioned action plan and supporting documentation available within the specified deadlines, this default shall be communicated to the Committee for its eventual actions, including the possibility of the imposition of an administrative penalty in terms of the FIAU's powers under Regulation 21 of the PMLFTR.

3 December 2020

APPEAL:

On Thursday 17th December 2020, the FIAU was duly notified that Insignia Cards Limited has, in accordance with the provisions of Article 13A of the Prevention of Money Laundering Act (PMLA), appealed the decisions taken by the FIAU. The Company has appealed all breaches as mentioned in this publication in relation to which the FIAU's Compliance Monitoring Committee decided to impose an administrative penalty. The Company appealed on the grounds that the FIAU failed to adequately analyse the information provided by the Company and also raised the issue as to whether the process that led to the imposition of this administrative penalty is in line with the right to a fair hearing. The quantum of the administrative penalty imposed is also being challenged by the Company.

22 December 2020

Pending the outcome of the appeal, the decision of the FIAU leading to the imposition of the administrative penalty is not to be considered final and the resulting administrative penalty cannot be considered as due, given that the Court may confirm, vary or revoke, in whole or in part, the decision of the FIAU. As a result, the FIAU may not take any action to enforce the administrative penalty pending judgement by the Court. This publication notice shall be updated once the appeal is decided by the Court to reflect the outcome of same.

4 August 2021