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 penalties 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:

13 April 2021

SUBJECT PERSON:

Money + Card Payment Institution Limited

RELEVANT ACTIVITY CARRIED OUT:

Financial Institution

SUPERVISORY ACTION:

On-site Compliance Review carried out in 2019.

DETAILS OF THE ADMINISTRATIVE MEASURE IMPOSED:

Administrative Penalty of €403,947 in terms of Regulation 21 of the Prevention of Money Laundering and Funding of Terrorism Regulations (PMLFTR).

LEGAL PROVISIONS BREACHED:

- Regulations 5(1) of the PMLFTR;
- Regulation 5(5)(a)(ii) of the PMLFTR;
- Regulations 7(1)(a), 7(1)(b) and 7(3) of the PMLFTR;
- Regulation 11(1)(b) of the PMLFTR;
- Regulation 7(1)(c) of the PMLFTR and Section 4.4.2 of the IPs;
- Regulation 11(5) of the PMLFTR;
- Regulations 13(1) and 13(2) of the PMLFTR;
- Regulation 15(1)(a) of the PMLFTR;
- Regulations 7(2)(a) and 7(2)(b) of the PMLFTR.

REASONS LEADING TO THE IMPOSITION OF THE ADMINISTRATIVE MEASURE:

Regulations 5(1) of the PMLFTR

The performance of a BRA became a legal requirement in January 2018. The Business Risk Assessment (BRA) provided by the Company was approved by the Board of Directors in the same month when the MFSA and the FIAU issued the Notification Letter in relation to the planned on-site compliance examination.

Meaning the Company carried out its BRA one year after the requirement to conduct it came into force. This despite the fact that the lack of a BRA was highlighted during an internal compliance audit conducted in August 2018.

It was noted that despite the content of the BRA covering the main pillars of risk factors, the knowledge of this assessment by the Company's senior officials was lacking. When questioned during the compliance review about any consideration taken in risk assessing the Company's operations, the MLRO and at times other company officials, were not always capable of answering the questions posed by the Officials. This lack of knowledge reaffirmed that the BRA made available during the compliance review was only a "paper-based" assessment documenting the risks to which the Company is or could be exposed. This, coupled with the lack of knowledge, hinders the effective implementation of controls aimed at mitigating such risks. Moreover, the examination revealed that there were different methodologies with which jurisdiction risk assessments were being carried out. This led to situations where the same jurisdiction was risk assessed in a different manner, depending on the methodology chosen.

The first document provided by the Company with a geographical classification was a document in which the scoring mechanism provided only the Basel AML Index rating for the different jurisdictions yet failed to indicate the risk factors for each of the jurisdictions. In addition, the Company produced a second document indicating a risk scoring of low, medium, or high for a number of jurisdictions the Company deals with highlighting those countries posing a higher risk. Yet how the two documents interlink to produce the Jurisdiction Risk Assessment (JRA) was not explained by the Company's officials. Nor was an explanation provided as to why two different documents with a number of jurisdictions being assessed twice through different methodologies was necessary.

Hence, in view of the aforementioned shortcomings the Company was found in breach of its obligations in terms of Regulation 5(1) of the PMLFTR.

Regulation 5(5)(a)(ii) of the PMLFTR

Customer Risk Assessment (CRA)

Despite the Company risk rating its clients through an 'AML Compliance Report Sheet', no documented policies and procedures that would guide the Company how to assess its customers were held. Therefore, how this report sheet was being completed (in particular how the Company arrived to the ultimate risk category of the customer) could not be understood. In the absence of specific guidance, the assessments could be said to be based on the subjective considerations of the Company officials. This in turn undermined a uniform and comprehensive assessment of all customers.

The Committee further noted that the CRA adopted by the Company was not rigorous and comprehensive enough to enable the Company to understand the risks posed by customers and to effectively apply the risk-based approach. Therefore, in view of the lack of identification of specific risks, the Company was not able to apply measures in order to mitigate the risks that the company would be exposed to by its customer during a business relationship. Moreover, the Company failed to provide a transparent, complete, and satisfactory view of the methodology it adopted to compute the various components of the customer risk assessment. This was evident through the review of documentation and interviews held with key individuals by FIAU officials.

Notwithstanding that the Company was risk rating its clients based on a number of criteria, it was observed that the risk assessment methodology applied held a set of parameters with inappropriate risk ratings. The

Committee expressed its concerns that the calculation of the formula used to aggregate the individual scores for each risk factor allowed for customers with similar profiles to be risk rated differently, without any rationale why such discrepancies were occurring. For example:

- Two customers forming part of the same structure and carrying out the same activity, while being ultimately risk rated the same, each risk factor substantially differed from one to another without any justification for such difference. It was observed that one customer was a Hong Kong company involved in advertising in the UK and was owned by a company located in Marshall Islands and owned a company in Panama. This customer was allocated a customer risk factor of 4 factor with the geographical risk scored at 4. On the other hand, another file (also a Hong Kong Company) also forming part of the same structure (thus exposed to the same jurisdiction risks) and offering the same services (advertising in UK) had a customer risk scoring of 9 and a geographical risk score of 9.

The Company's CRA model also did not adequately consider all the necessary key risk drivers which as a result impeded the Company from building a sufficient understanding of its customers' risk profile. This lack of detail also meant that the Company was not adequately capturing the degree of inherent risk emanating from its various client relationships. The deficiencies identified in this regard are being relayed hereunder:

- The CRA for 12 of the client files reviewed failed to incorporate an adequate geographical risk understanding since it did not take into consideration all the connected jurisdictions for each respective client (i.e., whether for example this related to the principal place of business, the country of incorporation or the country of birth of the Ultimate Beneficial Owner (UBO) amongst others). By way of example, the Committee considered that in one client file the Company failed to give weighting to the customer's targeted jurisdictions of operation which included Vietnam, Armenia, Azerbaijan, Belarus, Georgia, Kazakhstan, Kyrgyzstan, Moldova, Russia, Turkmenistan, Tajikistan, Uzbekistan and Asian Countries.

- The Committee learnt that following the review of a further 21 client files, it became evident that the 'AML Compliance Report' sheet lacked the consideration of the delivery channel or interface risk. This factor was a particularly important consideration for the Company in view that it on-boarded its customers mainly on a non-face to face basis.

The compliance examination also revealed 6 instances in which no information or documentation was held to confirm that the risk assessment had been carried out at all (i.e., both at the establishment of the business relationship and/or at on-going intervals). Consideration in this regard was given to the MLRO's explanation and confirmation that a risk assessment was not conducted since these clients were either employees of the Company or were employees of an external firm operating in the same premises as the Company at the time of the establishment of the business relationship. The Committee reiterated that the obligation to carry out a CRA is not dependent on the close relationship a subject person has with a customer and this in no way justified not carrying out a CRA in this regard. The obligation to carry out an adequate CRA and of documenting this assessment is equally applicable for all customers being serviced.

Revised Version of the Client Risk Assessment (March 2019 onwards)

Following the review of files and the newly introduced procedures, the Committee established that the Company still did not ensure a uniformity in the considerations taken when risk assessing customers.

Indeed, while the interface risk was included in the newly introduced procedure, it was not always taken into consideration. In 5 files where all customers were on-boarded on a non-face-to-face basis and who were on-boarded with the newly introduced system, the interface risk was not taken into consideration.

From the findings identified during the Compliance review and as confirmed by the Committee, the Company was far from understanding the ML/FT risks of its customers and in fact, no evidence was provided by the Company to show otherwise. Therefore, in view of the above considerations the Committee found the Company to have systemically breached Regulation 5(5)(a)(ii) of the PMLFTR.

Customer Acceptance Policy

Despite the Company's AML Compliance Manual indicating a number of non-acceptable jurisdictions with which the Company prohibits business relationships, 11 clients were identified as having connections with jurisdictions mentioned on the list. A number of relationships included a rationale as to why the Company proceeded to on-board the customer, making reference that the exposure is linked to the place of incorporation but not to target market or funds deriving from the same. However, this still contradicted the Company's own CAP. In addition, there were a number of other relationships which did not include a specific rationale for the deviation from their CAP the Company had adopted.

By way of example one customer had Algeria listed within its target markets, which jurisdiction was considered as a non-acceptable jurisdiction by the Company's CAP. In its rationale the Company's risk manager outlined that the relationship could still be accepted on the basis that the exposure was less than 1/4th a quarter of the Company's targeted markets and the customer was ultimately classified as medium high. The Committee however disagreed with the Company's conclusions and held that such exposure (which from the Company's statements can be said to be around 20% of the targeted market) was still to be considered as a significant exposure and surely not a one-off circumstance that would merit a deviation from its own policy.

Hence, in view of the aforementioned shortcomings the Company was found in breach of its obligations in terms of Regulation 5(5)(a)(ii) of the PMLFTR.

Regulations 7(1)(a), 7(1)(b) and 7(3) of the PMLFTR

The compliance examination revealed shortcomings by the Company in terms of its obligations which require the identification and verification of natural persons, legal entities and where applicable the UBO. From the file review, several shortcomings were noted in 12 customer files:

- The documentation obtained to verify the residential address of the UBOs and/or Agents for 5 customer files were invalid in terms of the requirements set out by the Implementing Procedures (IPs). This since the Company either obtained mobile utility bills or otherwise the documents were more than 6 months old at the time of on-boarding;
- In one customer file the document obtained to verify the residential address for the UBO did not match the address indicated in the customer's account opening form and no explanations were found on file explaining this conflicting information;
- In another file, the document obtained to verify the legal and ownership structure did not reflect the changes in the UBO shareholding structure which occurred prior to the establishment of the business relationship;
- 3 files having the same Beneficial Owner (BO) and also forming part of the same corporate structure, held various conflicting and contradictory information. Although sufficient information was obtained

to verify the legal structure for the holding company in order to establish the link with the BO, in the other two files the information and documentation obtained did not provide a confirmation as to who the BO is.

- In an additional 2 files, the link between the client and its BO could not be established as the corporate documentation was not collected. Both customers formed part of the same structure and were owned by the same BO.

Hence, in view of the listed shortcomings the Company was found in breach of its obligations in terms of Regulations 7(1)(a), 7(1)(b) and 7(3) of the PMLFTR for multiple failures to obtain the necessary identification and verification of natural persons and legal persons as required.

Regulation 11(1)(b) of the PMLFTR:

Notwithstanding the Company's policies and procedures referring to situations which by their nature represented a higher risk of ML/FT and thus warranted the carrying out of enhanced due diligence (EDD), the examination revealed that these were neither adequate nor effective in practice. This due to the fact that the Company failed to carry out the necessary EDD measures in 14 files reviewed albeit classifying the customer as high risk. For example:

- The business relationship for two customers commenced in July 2017 with accounts being opened in the name of two siblings residing and studying in Malta. The Source of Funding (SoF) to be passed through the accounts for both relationships was expected to be derived from their father's business who was involved in the selling of spare parts for cars, building materials, carpets, and furniture. Nevertheless, the Company failed to verify the financial standing of the father's business since no financial statements, or any other relevant documents were held on file. The Committee also noted that a google search conducted by the Company revealed that although the father was not a Politically Exposed Person (PEP), he still had some power and influence in Tajikistan. While the Company seems to have taken this into consideration when understanding the risks of the customer (since the customer was risk rated as high risk), there was no evidence of any enhanced measures being completed by the Company. Significantly the failure to carry out more thorough monitoring on the activities of the customer.

- The Committee noted that one corporate customer to which the Company offered a payment account with virtual IBANs for third party payments via SEPA was licensed in the Czech Republic as a Small Payment Institution. Notwithstanding the high anticipated level of activity (€36 million) to be carried out throughout the business relationship, the Committee observed that the Company did not obtain any further information nor supporting documentation in order to have a holistic understanding of the customer's business and risk profile. Therefore, the insufficient knowledge in relation to the customer's Source of Wealth (SoW) and SoF would hinder the Company from determining whether the transactions, both in volume and amount are in line not only with the nature of business but also in comparison to other institutions offering similar products and services within the industry.

  Moreover, the Company equally failed to apply any form of scrutiny on this customer. High volume of transactions conducted within one day which exceeded the €50,000 threshold were identified. This file held a business representation agreement between a related company and a counterparty which indicated that the client's account would be utilised to receive money from third parties. However, it

did not include the details as to the rationale for the receipt of payment. The Officials identified 37 transfers taking place during the period January to April 2019 between the client and the counterparty mentioned in the agreement accumulating to deposits of over €1.6 million. Following requests for supporting documentation, the Company only provided a Declaration of Source of Funds (DSF) form for six of the transactions which simply made reference to the aforementioned agreement. No further documentation was provided or made available to the Officials to support the remaining transactions.

Hence, in view of the aforementioned shortcomings the Company was found in breach of its obligations in terms of Regulation 11(1)(b) of the PMLFTR for its failure to carry out the necessary EDD measures that would address the higher ML/FT risk the customer was exposing the Company to.

Regulation 7(1)(c) of the PMLFTR and Section 4.4.2 of the Implementing Procedures

The compliance review revealed that the Company had failed on a number of occasions to adhere to its obligation to obtain sufficient information to establish the purpose and intended nature of the business relationships it maintained with its customers and to establish a comprehensive customer profile. As part of its deliberations, the Committee made the following considerations:

Employment/Business Activity:

- In 2 client files no information on the individuals' employment was held, but the application form only held information in relation to their prospective employment as introducers with the Company;
- In1 file pertaining to natural persons the Company officials limited themselves to obtaining information of a generic nature since the occupational details were listed as self-employed;
- The information collected for 6 corporate customers did not contain sufficient details on the business activity carried out since the Company only had reference to Media Consulting, Marketing Services and Sales Agency, thus again failing to obtain more concrete information as to the detail of the customers' activities.

Source of Wealth:

Throughout the compliance examination, 11 of the files analysed had inadequate information recorded to satisfy the (SoW). These files either had no information at all, or the information held on file did not provide enough detail to support the activities that generated the customer's wealth. This mostly because the Company was mainly focussing its resources on obtaining identification and verification details and documentation, which while important, on their own do not aid the Company to understand the customer and establish the customer's profile. Below are some of the considerations made by the Committee:

- In 1 file the Corporate activity was listed as 'an introducing broker' with the SoF to be derived through rebates from trading brokers they introduce clients to. The Company however did not understand how 'the introducing broker' would substantiate its activities such as the type of brokers they would target, including any contractual relationships and did not understand the customers being targeted since it only held information that customers are traders - this latter was considered to be too generic and may be associated with all kinds of corporate customers;

- In another file despite referring to the fact that the incoming transactions would be received from Dividends, the Company failed to obtain further information as to where such dividends will be derived from.

Consequently, the Company was not able to build a comprehensive business and risk profile about its customers prior to entering a business relationship with them. This profile would subsequently allow the Company to carry out effective transaction monitoring. For these reasons, the Committee found the Company to have failed to adhere to the obligations emanating from Regulation 7(1)(c) of the PMLFTR.

Regulation 11(5) of the PMLFTR

The compliance examination revealed that the Company did not obtain information on the PEP status for 4 client files reviewed as the PEP declaration field was either not listed in the application form or was left blank by the applicants. As a result, the Company was not in a position to determine whether its customer and/or the beneficial owner is a PEP and to thus allocate the necessary controls to counter such risks. This is required in order to be satisfied that the customer does not handle proceeds derived from corruption or other criminal activities which are increased risks known to be associated with customers who are PEPs.

Hence, in view of the aforementioned shortcomings the Company was found in breach of its obligations in terms of Regulation 11(5) of the PMLFTR.

Regulations 13(1) and 13(2) of the PMLFTR

Discrepancies in Client Lists:

In its Notification Letter, the Authority requested the Company to make available a complete list of both active and inactive customers. The Committee noted however that following the receipt of two client lists (initially with reference numbers and subsequently with client names) the Officials had deemed such lists to be inconclusive due to discrepancies being identified. Consequently, the Officials requested the MLRO to provide a third version of the client list however this list also held a number of clients with double profiles and included the 'clients of client' for one customer file that were not part of the information required by the officials onsite.

Secondly, despite being notified through the Authorisation letter issued by the FIAU not to inter alia destroy any information, the Officials identified that one Company representative had attempted to conceal documentation held at the Company's Office. When confronted about the incident, the representative in caption insisted that he was clearing his desk and was not aware that a client list was being destroyed. The Committee took note that when compared to the client lists previously provided it emerged that one client was not listed in the list provided to the Officials, and therefore the attempt to destroy the documentation raises suspicion that the Company official was trying to conceal the existence of the client.

Discrepancies in the Transaction Extracts:

While the Officials had requested the transaction history of the Company's customers, such transaction history proved to be incomplete and/or incorrect. This was due to the fact that following a high-level review, it was noted that a number of credit transactions were omitted from the system extract provided confirming that the list was not comprehensive. Several searches for transactions were conducted yielding negative results, leading officers to question whether the list of transactions in the initial extract was fully comprehensive.

Following additional queries, the second list of transactions was provided, with the Officials highlighting certain transactions which were not initially listed in the first extract. Additionally, the Officials identified a transaction that appeared to be an internal transfer between two accounts in the name of the same customer for the equivalent of €600. Following a review of all transactions with converted amount in

equivalence to €600, the Officials did not identify a matching transaction. Based on the above, the Officials concluded that the new system extract was also incomplete.

Matters were further exacerbated since when reviewing the transactional analysis, it was revealed that the Company did not retain any transactional data as recorded on the Company's former system and this was for the majority of the inactive clients. This was confirmed in 10 out of the 12 inactive client files reviewed for which the Company employees had limited access to account statements (only when a printed copy of same would be retained) and had to manually consolidate an excel sheet to retrieve transactions.

Access to the Subject Person's former systems and records:

The Company's AML Compliance Process Manual in which it was documented that "alerts are stored and can be easily retrieved from the system in the future". The Committee found this statement to be contradictory r to what was being carried out in the day-to-day operations. Upon reviewing the customer files, the Officials noted that the Company did not retain any alerts generated in relation to sanctions, PEP screening, adverse media and flagged transactions generated by the Siron KYC System. This since following its termination in 2017 the Company failed to retain any data previously held or to otherwise migrate same onto the new system (RDC). Furthermore, the Committee also noted how despite the MLRO indicating that the hits generated by the former system were constantly being reviewed, no justification or any other records were retained on file to explain why these hits were released/approved or otherwise. In addition, no detailed explanation of the review that the Company officials said they were carrying out was provided.

In view of all the above, the Committee considered that the failure of the Company to adhere to its record keeping obligations was systematic and was evident from the various considerations relayed above. The Committee therefore determined that the Company systematically breached Regulations 13(1) and 13(2) of the PMLFTR.

Regulation 15(1)(a) of the PMLFTR

The Committee observed that failures were identified in relation to all areas assessed by the Officials. What was more worrying was that a number of cases which necessarily merited further action by the MLRO were identified by the Officials. Nonetheless no action was taken by the MLRO. This due to the fact that the MLRO dedicating insufficient time to meet his obligations at law due to multiple appointments held (i.e. MLRO, Director, CEO, and Head of HR and Finance) combined with lack of knowledge of the AML/CFT obligations. The MLRO himself admitted that his knowledge and experience in relation to the local AML/CFT requirements was very limited and such statement was further re-affirmed as the queries raised by the officials were constantly being forwarded to other company officials for a reply.

Concerns were also raised since notwithstanding the MLRO having access to some of the records and data, he did not have sufficient knowledge and full access to all the Company's records. The explanations with regards to the newly introduced system, Policies and Procedures and all the data held on MacroBank (including customer information and transaction history) were being obtained solely from the Company's employees located in Prague, Czech Republic since the MLRO did not have direct access. This also raised concerns as to how adequately the MLRO carried out his duties when receiving internal suspicious reports, if he was not able to consider previous transactions, transaction patterns and volumes and previous instructions.

Therefore, after taking all of the above observations into consideration, the Committee found the Company in breach of its obligations in terms of Regulation 15(1)(a) of the PMLFTR.

Regulations 7(2)(a) and 7(2)(b) of the PMLFTR

Updating of Documentation/Information:

As part of its ongoing monitoring obligations, the Company was also required to update information in relation to customers. This should have been done both through the periodic review in terms of their policies and procedures (i.e., every six months irrespective of the client risk rating) and also for situations that impact on the business relationship (i.e. trigger events). It was noted however that this was not always being adhered to by the Company. By way of example:

- For 1 file, the Committee noted that approximately nine months after the commencement of the business relationship (around May 2018) there was a change in the corporate customer's name, however the Company had failed to update its records accordingly, at least up until the compliance review took place (i.e. April 2019).
- An additional 9 files held documentation to verify the identity and/or permanent residential address of the UBO/Agents/Applicants for business that had expired in the course of the business relationship and were not updated.

In addition, on-going monitoring record sheets were missing in a number of files; hence it could not be confirmed whether a review had been conducted by the Company in line with what the MLRO stated to be the Company's procedures for updating of customer information and documentation. The Committee took note of the unsigned "Due Diligence File Review – Ongoing monitoring" forms which were found for 16 clients, however this sheet mainly consisted of a checklist outlining the actions required for each client following the respective file review and could not be considered as proof to show that a review had been carried out.

Scrutiny of Transactions:

Serious shortcomings were identified in relation to the Company's obligation to scrutinise transactions taking place through the customers' accounts. The Committee considered that during the compliance examination minimal or no supporting documentation was held on file for a number of transactions reviewed. These transactions were either unusual or not in line with the information provided by the clients. Some examples are being outlined below:

- The documents on file for one customer indicated that the threshold set for the collection of documentation in relation to the SoF was adjusted to €50,000. However, the Officials were not provided with any invoice, agreement, or any other documentary evidence (nor any explanation) for three transactions which exceeded the stipulated threshold within a short period of time (€50,000 on 8 June 2018, €60,000 28 June 2018 and €50,122 on 2nd October 2018). When the account was closed, the remaining funds were transferred back to one of the counterparties from whom the client had received several incoming payments. The Officials noted that the closing transaction occurred on the same day in which a case was filed by the United States (US) District Court in relation to a securities fraud action, whereby the beneficiary (an unrelated company) and other counterparties were listed as defendants in the court case.

- In relation to another customer file, the client held a corporate current account together with a technical account linked with 27 PayBlock accounts. The activity through such accounts, in particular incoming transfers followed by immediate identical cash withdrawals from the same ATMs is not

customary to what would have been expected from a company involved in Marketing consultancy. Below are some examples that substantiate the Committee's concerns:

- the client received incoming payments amounting to €243,739.00 (without understanding the purpose for such receipt of funds) while €238,376.69 were withdrawn from both the clients' account and the sub-account holders respectively in the form of ATM withdrawals. None were queried by the Company;
- Between 14 August and 16 August 2018, 36 ATM withdrawals of amount €400 were conducted (Totalling €14,400) from two separate sub-account holder accounts, being withdrawn from the same ATM;
- Six ATM withdrawals of €4,000 each (Totalling €24,000) were conducted on 20 August 2018 from the same-mentioned two cards. Patterns of withdrawals continued to be observed throughout the business relationship where a total of 167 withdrawals were conducted from one card while 168 withdrawals were conducted from the other.

During a meeting between the Officials and the Company's MLRO and other Company Officials, the MLRO was unable to provide a hypothesis or any documentation to substantiate the patterns of the transactions reviewed. Further discussions with the MLRO revealed that the Company did not see any suspicion behind the clients' activity as it was stated that it is up to the client to decide how to utilise funds.

In view of the breaches outlined above to monitor the customer relationships and ensure that information and documentation held are up to date, as well as to have in place an efficient and adequate ongoing monitoring system that ensures the effective scrutiny of transactions throughout the course of the business relationships with its customers the Committee determined that the Company failed to honour its obligations in terms of Regulation 7(2)(b) of the PMLTFR.

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

After going into the merits of each finding as expressed above, the FIAU expressed its serious disappointment at the Company's total disregard to its AML/CFT obligations. This was clearly manifested through the lack of cooperation prior to the onsite examination taking place, in particular in failing to fully meet the requests by the FIAU for the provision of documentation in the manner and form that these were requested. The Committee was also concerned by the lack of commitment the Company had shown in understanding its AML/CFT obligations and in implementing measures to satisfy these obligations and in addressing the AML/CFT risks that the Company was or could potentially be exposed to. For these reasons, an administrative penalty of €403,947 has been imposed upon the Company.

In determining the final administrative penalty to impose, the Committee also took into consideration that Money + Card Payment Institution is no longer a licensed Financial Institution following the revocation of its license by the MFSA which came into effect on the 8 September 2019. It also considered the nature of the services and products offered by the Company and the size of its business operations. The Committee further considered that the obligations breached are important obligations and that these failures are serious and systematic in nature. The failures clearly demonstrate the limited regard the Company had towards the AML/CFT obligations applicable to its operations. The breaches listed could have an impact not only on the Company's own operations but also have repercussions on the local jurisdiction. The

Committee also considered that the Company was servicing customers without adequate AML/CFT safeguards in place, which could have led to the unintentional facilitation of money laundering.

20 April 2021

APPEAL:

On Friday 07 May 2021, the FIAU was duly notified that Money + Card Payment Institution 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 of wrong evaluation of facts 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.

14 May 2021