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 the subsequent appeals judgement. This Notice is not a reproduction of the actual decisions.

DATE OF IMPOSITION OF THE ADMINISTRATIVE MEASURE:

12 March 2019

SUBJECT PERSON:

Satabank plc (C66993)

RELEVANT FINANCIAL BUSINESS CARRIED OUT:

Credit Institution

SUPERVISORY ACTION:

On-site Compliance Review carried out in 2018

DETAILS OF THE ADMINISTRATIVE MEASURE IMPOSED:

The FIAU had initially imposed an administrative penalty of €3,711,300 in terms of Regulation 21 of the Prevention of Money Laundering and Funding of Terrorism Regulations (PMLFTR). This was revised by the Court of Appeal (Inferior Jurisdiction) to € 851,792.50.

LEGAL PROVISIONS BREACHED:

- Section 8.4 and Section 6.1 of the Implementing Procedures Part I (IPs);
- Section 4.1 and Section 8.1 of the IPs;
- Regulation 11(4)(a) and Regulation 7(9) of the PMLFTR and Section 4.1.1.1 of the IPs;
- Regulation 15(1), Regulation 15(6) and Regulation 15(8) of the PMLFTR and Section 6.4 of the IPs;
- Regulation 7(1)(a), Regulation 7(1)(b), Regulation 7(3)(c) of the PMLFTR and Sections 3.1.2, 3.1.1.2, 3.1.1.2(ii), 3.1.3.2, 3.1.3.3 and Section 3.2.5 of the IPs;
- Regulation 7(1)(c) of the PMLFTR and Sections 3.1.4 and 3.1.6 of the IPs;
- Regulation 10(2)(e) and Regulation 10(6) of the PMLFTR and Section 3.4.2 of the IPs;
- Regulation 11(1) of the PMLFTR and Section 3.5 of the IPs;
- Section 3.5.3 of the IPs; and
- Regulation 7(1)(d), Regulation 7(2)(a) and Regulation 7(2)(b) of the PMLFTR and Section 3.1.5 of the IPs.

REASONS LEADING TO THE IMPOSITION OF THE ADMINISTRATIVE MEASURE:

Internal Controls and Compliance Management Processes - Breach of Section 8.4 and Section 6.1 of the Implementing Procedures Part I

The Bank was found to be in breach of its obligations to establish adequate and appropriate internal controls and compliance management processes, by failing to allocate appropriate resources to the MLRO to monitor day-to-day operations of the Bank and by undermining the MLRO's influence over the Bank's AML/CFT policies and processes. These shortcomings prevented the Bank from adequately controlling and monitoring the implementation of its AML/CFT policies and procedures to ensure the Bank's services were not misused for ML/FT purposes.

While the Bank commissioned a number of AML audits and monthly AML compliance reports to review its CDD processes, it failed to take adequate action to address the shortcomings that were identified in these audits and reports. Indeed an AML audit commissioned in 2017 identified that out of 40 findings identified in a 2016 audit the Bank had only partially addressed 26 of the findings. The Bank deemed that the simple commissioning of the audits was sufficient to prove compliance with its AML/CFT obligations and that there was no need to take effective action on the resulting findings observed from said audits. Yet, the Bank failed to consider that the legal obligations require the policies and procedures to be adequately controlled and monitored.

Further accentuating the lax approach the Bank had towards enhancing its AML/CFT safeguards was its reaction to spot checks carried out by the Bank's compliance department, flagging out serious CDD deficiencies. Rather than ensuring the taking of timely and efficient actions to address the deficiencies flagged, the Bank opted to delay the remedial actions necessary and instead appointed independent auditors to re-evaluate the compliance department's findings. Concerns were heightened further since even following confirmation of the Compliance Department's findings by the independent auditors, the Board of Directors and Executive Management still did not take effective actions to ensure that all the identified shortcomings were efficiently and effectively remedied. The way the Bank acted in the face of clear identified weaknesses evidenced the Bank's lack of consideration to its AML/CFT obligations.

The Bank's inadequate internal controls and compliance management processes were also evident in the manner how two of its customer platforms were operated. Through these platforms, client relationships were being authorised by an outsourced service provider with the Bank, which was neither involved in nor in control of the on-boarding process. The Bank only had two relationship managers handling such platforms and they only held viewing rights over such portfolios. This modus operandi was not only clearly in breach of the Bank's AML/CFT obligations but also delayed substantially the execution of immediate actions, such as the blocking of transactions in case of suspicious activity as the Bank was completely dependent on action by the outsourced service provider. It was hence amply clear that the Bank was being utilised by the outsourced service provider as a vehicle for servicing clients without the Bank having any say over which type of clients to on-board and what CDD measures to employ.

The MLRO of the Bank was also not able to cause change within the Bank's AML/CFT processes, and in fact the MLRO's decisions were either being overruled or else questioned. Nor was the MLRO given sufficient resources to effectively safeguard the Bank's operations from ML/FT risks, and which resources were scarce both in terms of man power and also of systems. All this further contributed to negatively impact the Bank's ability to manage its compliance processes.

In view of the above-mentioned shortcomings, the Bank was found in breach of Section 8.4 and Section 6.1 of the Implementing Procedures Part I.

Risk Assessment and Risk Management Procedures – Breach of Section 4.1 and Section 8.1 of the Implementing Procedures Part I

Issues were also identified with respect to how the Bank was conducting its customer risk assessments. Shortcomings identified related to deficiencies in the manner in which risk assessments were conducted or related to cases where no customer risk assessments were carried out at all. While the Bank tried to link this obligation to the risk based approach, the Committee reiterated that the obligation to carry out a customer risk assessment for thorough understanding of ML/FT risks arising from its business relationships had been in force since the coming into force of the PMLFTR in 2008. In deliberating on the ensuing sanction measures, the Committee considered the materiality and importance of risk assessment obligations and the systematic implications of the shortcomings noted which had involved a widespread impact on the Bank's systems.

It was considered that no customer risk assessments were carried out to customers on-boarded through one of the Bank's platforms when the Bank started its operations in 2015. The Bank only introduced its customer risk assessment procedures in 2016. However even then, only two thirds of the customers on-boarded through this platform were eventually risk assessed, the other one third remained unassessed.

Additionally, although a new risk assessment system was introduced by the Bank in 2017, the methodology adopted within this system had a number of deficiencies including lack of consideration of product/service risk and interface risk and limitations in assessing geographical risk factors, resulting in inadequate risk assessments. Not factoring the product as one of the risk criteria had a significant bearing on the overall risk assessment and the risk rating assigned to each client, which could in turn impact the ensuing level of CDD to be applied. Similarly, the system failed to consider the interface through which customers were being on-boarded. Serious deficiencies were also identified with the Bank's assessment of geographical risks since jurisdictional risk ratings varied between customers depending on which platform they were being on-boarded even though the jurisdictions involved happened to be the same. This approach yielded different jurisdiction risk assessment scores depending on the client platform in question.

It was also noted that several customers had their business activity categorised as 'Professional Services' with no further detailed information. As a result, the Bank could not have formulated a clear picture of the risks actually posed by such customers, further evidencing the inadequacy of customer risk assessments carried out.

In view of the above-mentioned shortcomings, the Bank was found in breach of Section 4.1 and Section 8.1 of the Implementing Procedures Part I.

Customer Acceptance Policy (CAP) and providing services to a shell institution – Breach of Regulation 11(4)(a) and Regulation 7(9) of the PMLFTR and Section 4.1.1.1 of the IPs

In 2016, the Bank established a business relationship with a shell institution licensed in a non-EU jurisdiction. Although this was a single specific case, the relationship established was still in existence at the time of the compliance review and enabled the processing of a total credit turnover of €90.9 million by the end of 2017. Thus, the significance of this relationship in terms of the volume of funds transferred through and the ML/FT risks it exposed the Bank to could not be underestimated.

With the establishment of this relationship, the Bank was not only in breach of Regulation 11(4)(a) of the PMLFTR 2018 which clearly states that subject persons carrying out relevant financial business shall not continue correspondent relationships with shell institutions but it also went against the Bank's own CAP. The Bank tried to justify said relationship on the basis that a third party intermediary indicated that the shell institution was in the process of obtaining a licence. Yet the mere possibility of obtaining a licence could not be considered as a sufficient justification as at on-boarding and throughout the relationship with this customer it remained at all times a shell institution. The Committee thus determined that the Bank failed to ensure that a prospective applicant for business met the requirements of the Bank's CAP, hence breaching its obligations in terms of Regulation 7(9) of the PMLFTR and Section 4.1.1.1 of the IPs. Moreover, the Committee determined that the continued relationship with the shell institution breached the provisions of Regulation 11(4)(a) of the PMLFTR 2018. The duration of the relationship, which was still ongoing at the time of the compliance review, and the significant amount of funds processed through this relationship further accentuated the Committee's concerns.

In view of the above-mentioned shortcomings, the Bank was found in breach of Regulation 11(4)(a), Regulation 7(9) and Section 4.1.1.1 of the Implementing Procedures Part I.

Internal and External Reporting Procedures – Breach of Regulation 15(1), Regulation 15(6) and Regulation 15(8) of the PMLFTR and Section 6.4 of the IPs

A series of breaches of the Bank's reporting obligations varying in type and nature were identified. The most serious breaches consisted in failures to submit suspicious transaction reports (STRs) where suspicious activity was evident, failure to consider internally flagged suspicions to determine whether a STR should be submitted to the FIAU and submission of STRs well beyond the 5 working day deadline at the time provided for. In another number of instances, the Bank also failed to document the reasons why an internal suspicious report did not lead to an external report to the FIAU.

In respect of 7 customer, the Bank failed to submit a STR to the FIAU when it had sufficient grounds to do so. It was also noted that in 21 cases, the Bank blocked, terminated or placed under monitoring customer relationships in view of potentially suspicious activity, however no internal consideration was made by the Bank to determine whether a STR should be submitted to the FIAU, placing the Bank in breach of Regulation 15(6) of the PMLFTR. While the closure of accounts or business relationships with customers does not in itself require the submission of STRs to the FIAU, a report to the FIAU should be filed when said closure is due to suspicious activity linked to ML/FT.

In addition, the Committee also determined that in a number of instances, although STRs were submitted by the Bank, these submissions were done late, well beyond the 5 working days stipulated at law[1]. Out of 18 cases for which an internal report had been generated by Bank officials, the Committee deemed that 16 of these cases already included reasonable grounds to suspect ML/FT at internal reporting stage. Thus, an STR had to be submitted within 5 working days from the date when such 16 internal reports were filed. In these 16 cases, the Committee also considered the contents of the internal reports compared to the information submitted with the STR and noted that the MLRO added no value that could have justified why the STRs were not sent within the 5 working days from when the suspicion flagged in the internal

[1] It is being clarified that while the law in force at that time allowed for the submission of an STR within 5 working days from when the suspicion first arose, the current PMLFTR (see Regulation 15(3)) require the prompt submission of STRs supported with relevant identification and other documentation to the FIAU.

report first arose. It was also noted that the delay in sending the report for some of these 16 cases was extremely excessive.

In view of the above-mentioned shortcomings, the Bank was found in breach of Regulation 15(1), Regulation 15(6) and Regulation 15(8) of the PMLFTR and Section 6.4 of the IPs.

Identification and Verification of Customers and Beneficial Owners and ancillary obligations – Breach of Regulation 7(1)(a), Regulation 7(1)(b), Regulation 7(3)(c) of the PMLFTR and Sections 3.1.2, 3.1.1.2, 3.1.1.2(ii), 3.1.3.2, 3.1.3.3 and Section 3.2.5 of the IPs

Acquisition of customers from third parties

The Bank's acquisition of a portfolio of customers in 2015 from a financial institution licensed in another European country was carried out without any prior assessment of the AML/CFT procedures of the third party from whom the portfolio of clients was acquired. Such assessment was indispensable in order to determine whether the procedures of the financial institution satisfied, as a minimum, the obligations of the PMLFTR and IPs. In the absence of such assessment, the Bank did not even carry out CDD measures on a risk sensitive basis on the clients being acquired from the financial institution. Instead, it blindly took over a portfolio of clients with no AML/CFT checks whatsoever being undertaken. In addition, following a review of these client portfolios in 2016, gross deficiencies were identified in relation to compliance with Maltese AML/CFT obligations. Thus, although the Bank became aware of the widespread deficiencies and the risks it exposed itself to, it remained passive and never implemented any remedial actions.

In view of the above-mentioned shortcomings, the Bank was found in breach of Section 3.2.5 of the IPs.

Identification and verification of customers and ultimate beneficial owners

The Bank was found in breach of its obligations to identify and verify its customers appropriately, including the directors of corporate customers. Between 3% and 13.8% of personal customer files on-boarded and serviced through two platforms were not properly identified. Between 2.3% and 3.4% of the files reviewed for two platforms revealed improper identification of directors of corporate customers. In addition, 6.9% to 15.3% of the client files reviewed for two platforms held customers which were not appropriately verified.

In view of the above-mentioned shortcomings, the Bank was found in breach of Regulation 7(1)(a) and Regulation 7(3)(c) of the PMLFTR and Sections 3.1.1.2, 3.1.3.2 and 3.1.3.3 of the Implementing Procedures part I.

Failure to obtain the ownership structure of corporate customers and failure to properly identify and verify the ultimate beneficial owners of corporate customers

35.5% of customers reviewed for one of the platforms and 89.7% of customers reviewed for another platform did not have on file an ownership and control structure chart.

In addition, the majority of the corporate customer files on-boarded manifested shortcomings in the identification and verification of ultimate beneficial owners. Such failure was identified in 19.6% of the Bank's corporate customer files reviewed, in 82.6% of the files reviewed in relation to customers on-boarded through one of the Bank's platforms and in 89.7% of the files reviewed in relation to another of the Bank's platforms.

In view of the above-mentioned shortcomings, the Bank was found in breach of Regulation 7(1)(a) and Regulation 7(3)(c), Regulation 7(1)(b) of the PMLFTR and Sections 3.1.2, 3.1.3.2 and 3.1.3.3 of the Implementing Procedures Part I.

Translation of CDD documentation

Depending on the platform being used, this shortcoming was noted with respect to 100% to 24% of the documents that required translation. The Bank officials were thus not able to directly review and assess such documentation, whenever necessary, to carry out appropriate CDD such as effectively understanding the business activity and occupation of its customers to be able to monitor transactions effectively.

In view of the above-mentioned shortcomings, the Bank was found in breach of Section 3.1.1.2(ii) of the Implementing Procedures Part I.

Purpose and intended Nature of the Business Relationship – Breach of Regulation 7(1)(c) of the PMLFTR and Sections 3.1.4 and 3.1.6 of the IPs

The Bank was found deficient in collecting comprehensive information with respect to source of wealth, anticipated source of funds and business/employment activity of its customers at on-boarding. Thus the Bank was not able to properly establish the business and risk profile of its customers. Although the Bank had a 'Customer Source of Funds Declaration' form in place, it never made use of said form as instead it made use of another form consisting in a checklist which did not allow for information of any value to be collected. Moreover, in many instances information provided by said applicants did not include all the information required both in terms of law and in terms of the Bank's own Account Opening Procedure. In relation to two of the Bank's platforms, information on the customers' source of wealth and anticipated account turnover only started being requested by the Bank as from end July 2017, approximately two years after starting its operations in Malta.

The Committee also noted that from the client file sample review relative to the implementation of this obligation, the Bank demonstrated widespread and systematic non-compliance with the obligation to establish a comprehensive business and risk profile of its customers. Issues with the information collected was identified in 7.4% of the customer files reviewed as serviced from the Bank's different platforms which issues also reached up to 94.5% of the customers services through such platforms. This prevented the Bank from being able to understand the risks posed by customers and to ultimately determine whether they fell within the Bank's risk appetite. Moreover, in view of the widespread deficiencies in client profiling, it made it even more difficult for the Bank to be able to effectively monitor the transactions that took place within the established business relationships.

In view of the above-mentioned shortcomings, the Bank was found in systematic breach of Regulation 7(1)(c) of the PMLFTR and Sections 3.1.4 and 3.1.6 of the IPs.

Simplified Due Diligence (SDD) – Breach of Regulation 10(2)(e) and Regulation 10(6) of the PMLFTR and Section 3.4.2 of the IPs

The Bank applied SDD for e-money accounts offered to customers through two of its platforms. This meant that the Bank refrained from applying client identity verification measures until a transaction limit was reached (in line with its legal obligations). However, 35 of the customers to whom SDD was applied were found to have been allowed to continue transacting, even if the threshold had been exceeded, yet without the completion of due diligence being carried out. While the Bank argued that such failure was not

material, the Committee in determining the materiality of the breach, apart from the number of instances identified, also considered the intrinsic deficiency in the application of SDD for such e-money accounts. This due to the fact that the two platforms did not have an inherent or intrinsic transaction limit and that therefore the application of SDD could not have been effectively implemented for customers on-boarded through both platforms. Even more concerning, although the Bank did have an alert system that would generate reports when transactions using such products exceeded the €2,500 limit, client accounts were not being blocked until CDD had been completed, but rather clients could continue transacting beyond such limits.

Moreover customers on these two platforms were afforded a great deal of flexibility since they could easily open up to 50 and 25 accounts respectively and be provided with up to 5 debit cards per customer with each card having a daily withdrawal limited of €1,000. Since the Bank applied limits per card and not per customer, this meant that customers could easily increase said limited to €5,000 per day. This degree of flexibility substantially increased the risks for the Bank to being exposed to ML/FT, given that unverified account holders could in reality transact significant amounts of monies and thus the actual circumstances were not low risk ones which would allow the application of SDD. The Bank's argument that the finding was immaterial has been diametrically opposed and evidently unsubstantiated.

In view of the above-mentioned shortcomings, the Bank was found in systematic breach of Regulation 10(2)(e) and Regulation 10(6) of the PMLFTR and Section 3.4.2 of the IPs.

Enhanced Due Diligence (EDD) - Regulation 11(1) of the PMLFTR and Section 3.5 of the IPs

In all 10 cases for which clients were rated as high risk, the Bank completely failed to carry out the necessary EDD measures to mitigate the increased risk. Furthermore, although the Bank's policies require enhanced measures to be taken in case of higher risk customers, the policies and procedures lacked sufficient guidance as to what additional measures should be taken to cover the enhanced risks that the Bank was being exposed to.

It was therefore concluded that the Bank breaches its obligation to carry out EDD measures in all the cases classified as high risk by the Bank, indicating systematic issues with the application of EDD, which might be rooted in the Bank's policy not providing guidance on what EDD measures are to be applied when high risk situations are identified.

In view of the above-mentioned shortcomings, the Bank was found in systematic breach of Regulation 11(1) of the PMLFTR and Section 3.5 of the IPs.

Politically Exposed Persons (PEPs) – Breach of Section 3.5.3 of the IPs

The Committee also identified shortcomings in relation to the Bank's processes to determine whether customers and beneficial owners were PEPs. The Bank carried no PEP checks in relation to customers being offered a basic account on two of its platforms whereas in relation to corporate standard accounts, no PEP checks were carried out in 4.4% and 5.7% of customers. In addition customers and beneficial owners on-boarded by the Bank through another platform were not subjected to any PEP screening measures at all.

The Bank adopted a system whereby it would carry out checks on the PEP status depending on transactional limits imposed with respect to different type of accounts. While this approach had some merit in addressing possible ML/FT risks, it fell short of the actual requirement to check the PEP status which is independent of the transactions carried out. Moreover, and as already highlighted above, there

were serious issues with how the Bank was applying limits to its products and ensuring that these were not circumvented by its customers. Hence, even if the Bank's approach had any merit, its actual application diluted the same.

In view of the above-mentioned shortcomings, the Bank was found in systematic breach of Section 3.5.3 of the IPs.

Ongoing Monitoring – Breach Regulation 7(1)(d), Regulation 7(2)(a) and Regulation 7(2)(b) of the PMLFTR and Section 3.1.5 of the IPs

The Bank was found in breach of a number of serious and systematic shortcomings in its ongoing monitoring procedures. Applying effective ongoing monitoring of business relationships is considered to be a core and one of the most important AML/CFT obligations, enabling dubious, unusual and suspicious transactions and activities to be identified and reported. However, from the breaches identified, the Bank failed to appreciate the importance of such an obligation and to ensure effective ad comprehensive adherence to such obligation.

Ongoing monitoring was to a large extent being carried out manually by the Bank and in such monitoring, bank officials did not take into consideration the customer's AML/CFT risk, and important factors such as the customer type, industry type, remitter/beneficiary geographical location and account turnover, contrary to what the Bank's AML Policies and Procedures mandated. The Bank's automated processes did not assist in the assessment of transactions but rather in flagging transactions that exceeded certain transactional limits €50,000 (outgoing) and €250,000 (incoming). However, since the automated system was simply based on thresholds, the number of clients of the Bank and transaction volumes that took place still required extensive manual checks to analyse flagged transactions. Compounding the Bank's lax approach to its ongoing monitoring obligations, the Committee observed how transactions below the above-mentioned thresholds were not analysed, irrespective of volumes, timing and behavioural patterns.

Furthermore, the responsibility to review transactions and to analyse supporting documentation was vested with the payment analysts. However, such analysts were not even privy to the customer risk assessment results and the customer risk profile. Therefore, it could not be comprehended how such analysts could carry out the effective scrutiny of transactions. Another matter of concern was that where supporting documentation was being requested, at times the Bank was satisfied with a simple invoice or a basic agreement even though it was evident that such documentation would not explain the transaction being reviewed. Concerns on the supporting documentation obtained by the Bank were noted in instances ranging from 1.5% to 26.1% of the transactions reviewed, depending on the type of platform under review.

The Bank's ongoing monitoring systems also involved internal transfers being overlooked by the Bank which could have facilitated the layering of ill-gotten funds through various internal bank transfers between clients and accounts. In fact, these payments were not consistently subject to the same ongoing monitoring processes and controls applied to other payments and in the instances where supporting documentation was being requested by the Bank such documentation was still not being obtained.

The Bank adopted the practice to process all incoming transactions exceeding €50,000 but the value of which was less than €1,000,000 (subsequently lowered to €250,000 as from March 2017) by immediately crediting such funds into the customer accounts and requesting supporting documentation only afterwards, at times without taking any action when the supporting documentation requested would not be obtained. While in 2017 the Bank introduced a measure for blocking the accounts when supporting

documentation requested would not be received, this measure was ineffective since it could easily take various weeks from the initial receipt of funds before the account is actually blocked, allowing ample time for the funds to be transferred out of the Bank.

From discussions held with a senior member of staff of the Bank, it also became evident that the Bank did not request supporting documentation for transactions processed by the outsourced service provider's customers to whom the Bank supplied IBANs for e-money and payment accounts held by the service provider's customers. The Bank opted to apply SDD measures when monitoring these transactions and request information only on a random basis. This lack of proper monitoring is a fundamental deficiency in the Bank's control framework which exposed the bank to serious risks of ML/FT.

Customer account reviews

The Committee also noted that although the Bank's CAP dictated that although customer account reviews for all customers was to be carried out by September 2017, by the end of this year, the Bank had only carried out a review of 50 customer accounts (being the customers with the highest turnover on-boarded through one of its platforms). The Bank also failed to review customer accounts held by PEPs.

On the basis of the serious and concerning findings identified above, the Committee concluded that the Bank's ongoing monitoring systems were inefficient and ineffective and certainly not adequate to manage the Bank's ML/FT risks. The Bank was therefore found in systematic breach of Regulation 7(1)(d), Regulation 7(2)(a) and Regulation 7(2)(b) and Section 3.1.5 of the IPs.

CONSIDERATIONS TAKEN BY THE COMMITTEE AND ADMINISTRATIVE PENALTY IMPOSED:

Serious and concerning shortcomings of the Bank's adherence to its AML/CFT legal obligations have led to the imposition of the administrative penalty relayed hereunder. The findings of the compliance examination, apart from exposing very serious and systematic breaches of AML/CFT legal obligations by the Bank, shed light on the lack of commitment by the Bank and its administration to take AML/CFT requirements seriously. This lack of commitment is clearly manifested in the scarce resources dedicated to AML/CFT compliance and the MLRO, the improper ongoing monitoring tools and processes deployed and numerous cases of inaction in the wake of internal reports and audits which highlighted serious concerns with the application of AML/CFT obligations.

The Bank justified such serious and systemic failures on the basis that it was at the initial stage of its operations and that it took more time than originally anticipated to develop all systems, processes and procedures necessary. The Committee however disagreed with the Bank's statement that it was in the initial stages of its operations. At the time of the compliance review, the Bank had already been in operation for three years, during which time the Bank had established in excess of 150,000 customer accounts and in 2017 the Bank processed approximately 32 million transactions amounting to approximately €15 billion in value. The Bank should have thus ensured that it had the means and resources to appropriately manage the ML/FT it was exposed to from its business model and increased business influx. It is evident that the Bank's main consideration was that of enhancing its business operations without strengthening its AML/CFT controls proportionately.

The FIAU is also concerned with the repercussions that the lax attitude adopted by the Bank towards it obligations to implement effective, efficient and comprehensive AML/CFT controls had on the jurisdiction as a whole. The Bank serviced various financial intermediaries and enablers that used the Bank's accounts that were subject to lax and at times inexistent AML/CFT safeguards to transfer significant volumes of monies, exposing not only the Bank itself to risks of ML/FT but also exposing the jurisdiction as a whole.

In determining the administrative penalty to be imposed, the Committee took into consideration for each failure identified: the importance of the obligation breached, whether the failures were visible and continued for a prolonged period of time, the limited and ineffective remedial actions taken by the Bank, whether breaches were the result of deliberate or negligent practices and the impact the failure had on the local financial sector and the jurisdiction.

The Committee found the Bank to be in serious and systemic breach of various AML/CFT provisions and on the basis of all the above-mentioned considerations decided to impose an administrative penalty of €3,711,300 (three million, seven hundred eleven thousand and three hundred euro) in terms of Regulation 21 of the PMLFTR.

APPEALS PROCESS:

In accordance with the provisions of Article 13A of the Prevention of Money Laundering Act (PMLA), the Bank appealed the respective decisions taken by the FIAU on the imposition of the administrative penalty for the Bank's failure to adhere to its AML/CFT obligations. Separate proceedings were filed on behalf and in the name of the Bank by the Bank's appointed competent person and by the Bank's shareholders.

By means of the decisions handed over on the 15 December 2020 and communicated in full to the FIAU on 16 December 2020, the Court of Appeal:

a) Declared the appeal filed by the Bank's shareholder to be null and void as the Bank could not file two appeals for the same decision and judicial representation in the case of administrative fines vested exclusively in the Competent Persons that had been appointed.
b) In the appeal proceedings filed by the Competent Person upheld the determination as to the breaches committed by the Bank, including their serious and systemic nature but revised the administrative penalty to €851,792.50

While the Court acknowledged that Regulation 21(4) of the PMLFTR allowed significant discretion as to the amount of the administrative sanction to impose in the case of serious, repeated and systemic breaches, it also considered that the amount should be such as to adhere to the respective thresholds set out in this provision. Moreover, the Court also considered that the exceptional circumstances present in this case had to be taken into account when reaching a decision as to the quantum of the administrative penalty to be imposed.

23 December 2020