SAINT CHRISTOPHER AND NEVIS

STATUTORY RULES AND ORDERS

No. 41 of 2020

Saint Christopher and Nevis Financial Services (Implementation of Industry Standards) (Amendment) Regulations, 2020

In exercise of the powers conferred by section 52 of the Financial Services Regulatory Commission Act, Cap. 21.10, the Minister makes the following Regulations

[Published 3rd September 2020, Extra Ordinary Gazette No. 69 of 2020]

1. **Citation.**

These Regulations may be cited as the Financial Services (Implementation of Industry Standards) (Amendment) Regulations, 2020.

2. **INTERPRETATION**.

In these Regulations, unless the context otherwise requires, the expression, "Regulations" means the Financial Services (Implementation of Industry Standards) Regulations, No. 51 of 2011.

3. **AMENDMENT OF REGULATION 2.**

The Regulations are amended in regulation (2) by inserting in the correct alphabetical order, the following expressions:

" "proliferation financing or "PF" has the meaning assigned to it in regulation 7;

" "UNSCR" means United Nations Security Council Resolution.".

4. **AMENDMENT OF REGULATIONS.**

The Regulations are amended as follows by replacing the expression:

(a) "Anti-Terrorism Act, 2002", wherever it occurs with the expression, "Anti-Terrorism Act, Cap. 4.02";

(b) "Financial Services Regulatory Commission Act, 2009", wherever it occurs, with the expression, "Financial Services Regulatory Commission Act, Cap. 21.10";

(c) "Financial Intelligence Unit Act, 2000", wherever it occurs, with the expression, "Financial Intelligence Unit Act, Cap. 21.09";

(d) "National Council on Drug Abuse Prevention Act, 2000", wherever it occurs with the expression, "Drugs (Prevention & Abatement of the Misuse and Abuse of Drugs) Act, Cap. 9.08;

(e) "Organised Crime Prevention and Control Act, 2002", wherever it occurs, with the expression, "Organised Crime Prevention and Control Act, Cap. 4.22";

(f) "Proceeds of Crime Act, 2000", wherever it occurs with the expression, "Proceeds of Crime Act, Cap. 4.28;

5. **AMENDMENT OF SCHEDULE - PARAGRAPH 10.**

The Schedule to the Regulations is amended in paragraph 10 by replacing it as follows:

" 10. **GROUP-WIDE AML/CFT PROGRAM**

This section applies to a regulated business that has branches or majority-owned subsidiaries or agents anywhere in Saint Kitts and Nevis or outside Saint Kitts and Nevis.

(a) A regulated business and any of its branches, subsidiaries or agents must not open accounts, provide services or establish business relationships with a customer unless the regulated business has established and continues to maintain an adequate AML/CFT policies and procedures manual.

(b) A regulated business must implement its AML/CFT group-wide policies and procedures manual and update it as required to take into account new and emerging risks, trends and updated legislation.

(c) The AML/CFT group-wide policies and procedures manual of a regulated business must have regard to:

(i) the nature and level of ML/TF risks that all branches, majority-owned subsidiaries and agents of the regulated business may reasonably expect to face in the course of their business; and

(ii) the nature, size and complexity of such businesses.

(d) The AML/CFT group-wide policies and procedures manual of a regulated business must contain group-wide policies, processes and procedures as follows:

(i) that are applicable and appropriate to all branches, majority-owned subsidiaries and agents of the regulated business;

(ii) that cover the requirements of paragraphs 23 to 40;

(iii) on the sharing of information amongst all branches, majority-owned subsidiaries and agents of the regulated business for the purposes of customer due diligence, and AML/CFT risk management;

(iv) for all branches, majority-owned subsidiaries and agents of the regulated business to provide customer account and transaction information to each other including information and analysis of transactions or activities which appear unusual; and

(v) that contain adequate safeguards on the confidentiality and use of information shared, including safeguards to prevent tipping-off;

(e) If a branch, subsidiary or agent operates in a foreign country, the branch, subsidiary or agent must apply the AML/CFT group-wide policies and procedures manual;

(f) A regulated business must make available a copy of its AML/CFT group-wide policy and procedures manual to the Commission upon request made to it in writing by the Regulator/Director;

(g) A regulated business must ensure that its foreign branches and majority-owned subsidiaries apply AML/CFT measures consistent with the requirements of St. Kitts and Nevis, where the minimum AML/CFT requirements of the host country are less strict than those of St. Kitts and Nevis;

(h) If the host country does not permit the proper implementation of AML/CFT measures consistent with the requirements of St. Kitts and Nevis, the regulated business must apply appropriate additional measures to manage the ML/TF risks and inform the Commission.

6. AMENDMENT OF SCHEDULE - PARAGRAPH 18

The Schedule to the Regulations is amended in paragraph 18 by inserting the following new paragraphs immediately after paragraph 18 (b) (ii) as follows:

" 18A. THE RISK-BASED APPROACH TO ANTI-MONEY LAUNDERING AND COUNTERING THE FINANCING OF TERRORISM (AML/CFT) AND COMBATING PROLIFERATION FINANCING (CPF)

(1) Overview:

(a) This part provides guidance on how to carry out a risk assessment of the business.

(b) Regulated businesses must assess the risk that they could be used for money laundering (ML) and terrorist financing (TF) and the financing of the proliferation of weapons of mass destruction (PF).

(c) Regulated businesses must decide which areas of the business are at risk and implement measures to prevent ML/TF/PF by using what is known as a 'risk-based' approach (RBA).

(d) Regulated businesses must adopt an RBA for dealing with ML/TF and proliferation of weapons of mass destruction threats. RBA means that a regulated business is expected to identify, assess and understand the ML/TF/PF risks to which it is exposed and to take measures that are commensurate with those risks in order to mitigate them effectively.

(e) The RBA is not optional, but a prerequisite for the effective implementation of anti-money laundering, counter terrorist financing and counter proliferation financing measures. For that reason, the risk assessment must be subject to ongoing monitoring and kept up to date.

(f) The RBA must be documented and made available to the Board of Directors, senior management and other relevant personnel for consideration and appropriate action. Copies of the documented RBA must also be made available to the Commission and other Competent Authorities, upon request.

(g) The documented RBA must be approved by the Board of Directors and periodically reviewed to determine any changes in risk exposure or risk appetite.

(h) Where ML/TF/PF risks are higher, regulated businesses have to take enhanced measures to mitigate the higher risks. The range, degree, frequency or intensity of control used should be stronger. Where the ML/TF/PF risk is identified as lower, AML/CFT/CPF measures may, under certain conditions, be reduced, which means that each of the required measures has to be applied, but the degree, frequency or the intensity of the controls used will be lighter or simplified. This may be done where the regulated business has controls in place that reflect the degree of risk of ML/TF/PF identified as well as adequate measures to monitor the effectiveness of implementation of those controls to the standard required.

(i) In assessing its own risk, a regulated business shall take into account:

  (i) the results of the National Risk Assessment (NRA) of Saint Kitts and Nevis and any other jurisdiction in which it operates, taking account of the requirements in place, noting any legally prescribed areas of high or significant risks, and legally permitted mitigating measures for low risk;

  (ii) results of examinations conducted by the Commission and feedback from the Commission;

  (iii) internal policies and procedures;

  (iv) laws and regulations which govern the regulated business;

  (v) any relevant internal and external information;

  (vi) mutual evaluation reports; and

  (vii) typologies.

(j) Where risks are high, regulated businesses shall always use enhanced due diligence, even if mitigation measures are not set out in law.

(k) Simplified measures may not be used by a regulated business where a suspicion of ML/TF/PF exists.

(l) Assessing and understanding risk requires skilled and trusted staff. Where appropriate, staff should be assigned "fit and proper" tests to assess their knowledge level. They should be technically equipped to carry out their tasks, commensurate with the complexity of the operations.

(2) Advantages of the risk-based approach

Regulated businesses are able to decide on the most cost-effective way to control the risks of money laundering, terrorist financing and proliferation financing when the steps involved in the risk-based approach are followed. This allows the regulated business to focus its efforts and resources where the risks are highest. A risk-based approach would also assist the Board of Directors and Senior Management of the regulated business with the following:

(a) managing and understanding the business' risk exposure;

(b) establishing a risk appetite;

(c) identifying weaknesses in internal controls; and

(d) establishing a strategic plan and decision making.

(3) The risk-based approach – enterprise-wide risk assessment

(a) Regulated businesses shall use a risk-based approach to prevent ML/TF/PF. This involves following a number of steps:

(i) identifying the ML/TF/PF risks that are relevant to the business;

(ii) carrying out a detailed risk assessment of the business, focusing on customer risk assessment, new and existing products and services, delivery channels, geographical location, etc.;

(iii) assessing the levels of bribery and corruption affecting the business;

(iv) designing and putting in place controls to manage and reducing the impact of these risks;

(v) monitoring implementation of the controls and improving their efficiency, where necessary;

(vi) keeping records of what was done and why it was done; and

(vii) carrying out re-assessments at appropriate intervals based on the residual risks determined. Some regulated businesses may refresh their risk assessments annually, however, if there are no material changes to the risk environment or high-risk areas which require enhanced monitoring and assessment, some businesses may choose to undertake their risk assessments less frequently. In exceptional circumstances, such as regulatory intervention for example, a risk assessment may be conducted more frequently than annually.

(viii) ensuring that a risk assessment that is carried out is properly documented, maintained and communicated to relevant personnel, senior management and the Board of Directors.

(4) **How to carry out an enterprise-wide risk assessment**

(a) A regulated business must decide how to carry out its own risk assessment which may be simple or complex depending on the:

(i) size and structure of the business;

(ii) geographical location of the business;

(iii) regulatory framework of the jurisdiction where the business operates from;

(iv) range of activities the business carries out; and

(v) nature of the products and services it supplies.

(b) In assessing the risks of ML/TF/PF that apply to the business, the regulated business needs to consider and understand:

(i) the results of the customers' risk assessment (see Paragraphs 34 – 37);

(ii) the results of the product risk assessment;

(iii) the delivery channels and payment processes, for example cash over the counter, cheques, electronic transfers, virtual or digital currency or wire transfers;

(iv) its branches and subsidiaries and the jurisdictions which these operate from; and

(v) the policies, procedures and internal controls in place.

(5) **Identifying inherent ML/FT/PF risks**

(a) A regulated business should start identifying its inherent ML/FT/PF risks by reviewing the results of the country's NRA and what particulars it provides in relation to the country, regulated businesses and the financial sector of which its business is a part.

(b) In identifying the ML/FT/PF risks to which it is exposed, a regulated business must consider and understand a range of factors, including the:

(i) nature, scale, diversity and complexity of the business;

(ii) target markets;

(iii) inherent risk of products and services offered;

(iv) number of customers already identified as high risk;

(v) jurisdiction it is exposed to either through its own activities or the activities of customers, especially jurisdictions that are subject to advisories for being high risk or having strategic AML/CFT deficiencies or for which countermeasures have been called for by FATF, the international or regional oversight bodies;

(vi) regulatory framework of the jurisdiction that the regulated business operates from;

(vii) degree to which it relies on third parties to conduct elements of customer due diligence;

(viii) distribution channels; and

(ix) use of technology including new and developing technologies.

(c) It is useful to categorise risks to better understand and prioritise them. Categorisation is usually on a scale of "High–Medium–Low". A scoring

system may also be used (eg. 1, 2, 3) for each factor examined. Once each factor is examined, an overall score is calculated to the risk of low, medium or high based on established categories. The regulated business must also consider the materiality of each risk factor identified for the business and its operations.

(6) **Assessing the risk management systems of the regulated business**

The regulated business must assess the adequacy and effectiveness of its internal controls and risk management systems. The following aspects shall be considered and understood:

(a) the compliance function, including capacity, adequacy and capability of the Compliance Officer and support staff;

(b) the adequacy and effectiveness of the following:

(i) AML/CFT policies and procedures of the regulated business, including training, record keeping, monitoring, reporting of suspicious transactions and related matters;

(ii) risk assessments conducted on customers, goods and services.

(ii) the internal audit function.

(c) the role of senior management and the Board of Directors and their oversight over the internal controls;

(d) organisational structure and the operational software and database; and

(e) results of examinations conducted by the Commission.

(7) **Determine the overall risk of the regulated business**

(a) The regulated business must consider the overall results of the assessment of the inherent risks.

(b) The risk management systems and internal controls should be assessed to determine the overall adequacy and effectiveness to manage and mitigate the inherent risks. The size, structure and complexity of the regulated business should be assessed when determining adequacy and effectiveness of internal systems and controls.

(c) Once the overall inherent risks and the adequacy and effectiveness of the internal systems and controls have been assessed, the regulated business must determine the residual risk (overall risk). This can be determined by using a scoring system or through categorization (low, medium, high).

(d) The overall risk rating results should be analyzed in conjunction with the documented RBA and risk appetite to ensure that the results are in accordance with these.

(e) Based on the overall risk rating, the regulated business should determine the intervals in which subsequent risk assessments should be conducted. A high overall risk requires frequent re-assessment to reduce the risk to be in accordance with the regulated business' risk appetite. In such cases,

recommended actions or internal policies should be improved or developed to reduce the high-risk rating. The recommended actions can include:

(i) updating policies and procedures including Know Your Customer (KYC) procedures;

(ii) increased training;

(iii) reviewing of risk assessment procedures for customers, products and services;

(iv) conducting a risk-based internal audit to identify weaknesses;

(v) improving enhanced due diligence and monitoring procedures; and

(vi) improving suspicious transaction reporting.

(f) The results of the enterprise-wide risk assessment along with recommended actions, if any, should be communicated to senior management and the Board of Directors. The recommended actions should include a timeline for completion.

(g) The Board of Directors shall review and approve the enterprise-wide risk assessment along with the recommended actions. A follow-up risk assessment should be conducted to verify the effectiveness of the recommended actions to reduce the high risk rating. Re-assessment should continue to take place until the approved risk appetite is obtained.

(h) Notwithstanding the intervals determined by the results of a risk assessment, the following should prompt a risk assessment:

(i) changes in the nature of business;

(ii) introduction of new business or services;

(iii) growth through mergers and acquisitions

(iv) entry into new markets; and

(v) results of the country's NRA.

(8) **Product Risk Assessment**

(a) A regulated business should conduct product risk assessments in the following instances:

(i) the introduction of new products to the business; and

(ii) where there have been any changes in existing products.

(b) The following steps should be taken as part of product risk assessment:

(i) The regulated business should identify the following inherent risks:

(A) characteristics of the product;

(B) performance of the product;

(C) the market that the product is delivered or provided to;

(D) Delivery channels of the product

(ii) Assess the risk management processes in place to reduce the inherent risks

(iii) Determine the overall residual risk. This can be completed through categorization or a scoring system.

(c) Based on the risk rating, the regulated business must decide the manner in which the product would be monitored or whether to proceed with the product.".

7. AMENDMENT OF SCHEDULE - PARAGRAPH 22.

The Schedule to the Regulations is amended by inserting immediately after paragraph 22, the following new paragraphs:

" **PROLIFERATION FINANCING.**

(1) Proliferation financing means the act of providing funds or financial services which are used, in whole or in part, for the

(a) manufacture;

(b) acquisition;

(c) possession;

(d) development,

(e) export,

(f) trans-shipment,

(g) brokering,

(h) transport,

(i) transfer,

(j) stockpiling;

(k) or use

of nuclear, chemical or biological weapons and their means of delivery and related materials, including both technologies and dual use goods used for non-legitimate purposes, in contravention of national laws or, where applicable, international obligations.

(2) The following elements may be indicators of proliferation financing where:

(a) a transaction involves a person or entity in a foreign country of proliferation concern;

(b) a transaction involves a person or entity in a foreign country of diversion concern;

(c) the customer or counter-party or the address of the customer or counter-party is similar to one of the parties found on publicly available lists of "denied persons" or has a history of export control contraventions;

(d) the customer activity does not match the business profile, or the end-user information does not match the end-user's business profile;

(e) a freight forwarding firm is listed as the product's final destination;

(f) an order for goods is placed by firms or persons from foreign countries other than the country of the stated end-user;

(g) a transaction involves shipment of goods incompatible with the technical level of the country to which it is being shipped, for example, where semi-conductor manufacturing equipment is being shipped to a country that has no electronics industry;

(h) a transaction involves possible shell companies;

(i) a transaction demonstrates links between representatives of companies exchanging goods, such as the same owners or management;

(j) a circuitous route of shipment is used where a more direct one is available or a circuitous route of financial transaction is used;

(k) a trade finance transaction involves a shipment route through a country with weak export control laws or weak enforcement of export control laws;

(l) a transaction involves persons or companies, particularly trading companies, that are located in countries with weak export control laws or where there is weak enforcement of export control laws;

(m) a transaction involves shipment of goods inconsistent with normal geographic trade patterns, for example where the country involved does not usually export or import the goods involved;

(n) a transaction involves financial institutions with known deficiencies in AML/CFT controls or where those institutions are domiciled in countries with weak export control laws or where there is weak enforcement of export control laws;

(o) based on the documentation obtained in transaction, the declared value of a shipment is clearly under-valued in respect of the shipping costs;

(p) inconsistencies in information contained in trade documents and financial flows, such as names, companies, addresses, final destination and other basic information;

(q) a pattern of wire transfer activity shows unusual patterns or has no apparent purpose;

(r) a customer provides vague or incomplete information and is resistant to providing additional information when required;

(s) a new customer requests a letter of credit while still awaiting the approval for an account to be opened which would form the backing or guarantee for the letter of credit;

(t) there is a request for wire instructions or a payment is made to or from parties who were not identified on the original letter of credit or other documentation.

(3) The following are additional potential indicators of sanctions evasion activity mentioned in third-party reports such as the United Nations Panel of Experts Report or other academic research, where there is:

(a) the involvement of items controlled under Weapons of Mass Destruction (WMD) export control regimes or national control regimes;

(b) the involvement of a person

(i) connected with a country of proliferation concern for example a dual-national; or

(ii) with complex equipment for which he or she lacks the technical background;

(c) the use of cash or precious metals such as gold in transactions for industrial items;

(d) the involvement of a small trading, brokering or intermediary company, carrying out frequent business transactions that are inconsistent with the normal business of that company;

(e) the involvement of a customer or counter-party, declared to be a commercial business but whose transactions suggest that they are acting as a money-remittance business;

(f) a record of transactions between companies on the basis of "ledger" arrangements that obviate the need for international financial transactions;

(g) an indication or evidence that customers or counterparties to transactions are linked through the sharing of a common physical address, IP address or telephone number, or that there is collusion, collaboration or coordination of activities, whether criminal activities or otherwise, between those customers or counterparties;

(h) involvement of a university in a country of proliferation concern;

(i) description of goods on trade or financial documentation is non-specific, innocuous or misleading;

(j) evidence that documents or other representations relating to shipping, customs, payment or other relevant information, are fake or fraudulent;

(k) the use of a personal account to purchase industrial items.

8. **AMENDMENT OF SCHEDULE - PARAGRAPH 23**

The Schedule to the Regulations is amended in paragraph 23 by replacing the expressions, "training (see paragraphs 131 – 134)" and "recruitment and supervision of staff", occurring in the fifth and sixth bullet points, with the expression, "**training, recruitment and employee screening (see paragraphs 131 – 134)**".

9. **AMENDMENT OF SCHEDULE - PARAGRAPHS 24 - 27**.

The Schedule to the Regulations is amended in paragraphs 24 to 27 by replacing those paragraphs as follows:

" AML/CFT/CPF POLICIES AND PROCEDURES MANUAL

24. A regulated business must not open accounts, provide finance business or financial services or related products or establish a business relationship with a customer unless the regulated entity has established and maintained an adequate AML/CFT/CPF policies and procedures manual that has been approved by its Board of Directors or its principals.

25. A regulated business must implement its AML/CFT/CPF policies and procedures manual and update it as required to take into account new and emerging risks and amendments to relevant legislation. The manual must have regard to:

    (a) the nature and level of ML/TF/PF risks that the regulated business may reasonably expect to face in the course of its business;

    (b) the legislative requirements; and

    (c) the nature, size and complexity of the business and regulated business.

26. The AML/CFT/CPF policies and procedures manual must contain internal policies, processes and procedures:

    (a) to implement the customer due diligence requirements of regulations 4, 5, 6 and 7 of the Anti-Money Laundering Regulations and the Anti-Terrorism (Prevention of Terrorist Financing) Regulations;

    (b) to implement the reporting requirements under regulation 11 of the Anti-Money Laundering Regulations and the Anti-Terrorism (Prevention of Terrorist Financing) Regulations;

    (c) to implement the record keeping requirements under regulations 8 and 9 of the Anti-Money Laundering Regulations and the Anti-Terrorism (Prevention of Terrorist Financing) Regulations;

    (d) to inform the regulated business' officers and employees of the laws of Saint Kitts and Nevis related to the policies, processes, procedures and systems adopted by the regulated business to mitigate against ML/TF/PF;

    (e) to train the regulated business' officers and employees to recognize and deal with ML/TF/PF and monitor accordingly;

    (f) to vet the officers and employees of the regulated business to ensure that they are fit and proper persons to engage in AML/CFT/CPF related duties;

    (g) on the appropriate documents to be collected and maintained during the recruitment of new officers and employees;

(h) on the role and responsibility of the Compliance and Reporting Officers;

(i) on the establishment of an audit function which is able to test its AML/CFT/CPF processes, procedures and systems;

(j) on the adoption of systems by the regulated business to deal with ML/TF/PF; and

(k) on systems and mechanisms to monitor the behaviour and transactions of customers for unusual or suspicious activities.

27. A regulated business must periodically engage an external auditor to provide an independent review of its AML/CFT/CPF processes, procedures and systems, and to make recommendations for improvements.".

10. **AMENDMENT OF SCHEDULE - PARAGRAPH 28.**

The Schedule to the Regulations is amended in paragraph 28 by inserting immediately after that paragraph, the following new paragraphs:

" 28A (a) ***Independent Audit***

The ultimate objective of an independent audit is to provide an independent analysis of the operations of the regulated business. By conducting an independent audit, the regulated business can improve its processes and operations by identifying weaknesses in its internal systems and controls which would in turn assist the Management of the regulated business in developing suitable policies and procedures.

(b) ***Key Features of the Independent Audit Function***

The regulated business may choose to have the service of the independent audit function provided fully from within the organisation, outsourced to an external auditor or through a combination of internal and external sourcing. The key is to ensure that all individuals involved in this function are independent in *"fact"*. Individuals who are performing this function should therefore not be involved in the day-to-day operations of the business. The following key features are essential for the effective operation of an independent audit function:

(i) Independence and objectivity—The independent audit function must be independent of the activities being assessed, which requires the function to have sufficient autonomy and authority within the institution, thereby enabling the auditors to carry out their assignments with objectivity.

(ii) Professional competence—The knowledge and experience of the auditors are essential components to ensure the effectiveness of the independent audit function.

(iii) Professional ethics—Independent auditors must act with integrity. The regulated business must ensure that the auditors are appropriately vetted.

(iv) The independent audit charter—The regulated business should have an independent audit charter that articulates the purpose, standing and authority of the independent audit function.

(v) The independent audit should be conducted in accordance with the risk management policies of the regulated business and be reviewed on a regular basis by the Audit Committee or Senior Management. In the performance of this function, the independent auditors should adopt a risk-based approach where the weaknesses identified are reviewed and monitored in a frequency and manner that reduces or maintains the regulated business' risk appetite.

(c) ***The Audit Charter***

The Independent Audit's Charter should provide clarity about its:

(i) strategy and objectives;

(ii) role and responsibilities within the regulated business;

(iii) scope of work;

(iv) accountability to the audit committee or management;

(v) reporting lines for line management purposes;

(vi) unfettered access to all information, people and records across the regulated business;

(vii) independent audit function so that the Independent Auditor shall not be involved in the day-to-day operations being audited where it has to review its own work.

(d) ***Steps of an Independent Audit***

Plan: An audit plan should be developed. This plan should include a risk-based approach and should be approved by the Audit Committee or Senior Management.

Notify: The relevant persons (department heads, supervisors and similar management personnel) should be notified of the audit along with the duration of the review.

Test: The tests should include interviews with employees, reviews of policies, procedures and systems and an assessment of the internal controls.

Prepare Draft Report: The report should outline the audit scope and objectives, a summary of the audit process, findings and recommended actions to rectify deficiencies.

Management's Response: Management should review the draft report and provide feedback and a suitable timeframe for the completion of the recommended actions.

Final Report: The final report should be prepared with the Management's Response and the follow-up process to review the implementation of recommended actions.

Review by Board of Directors/Senior Management: The final report should be reviewed and approved by the Board of Directors/Senior Management.

Follow-up: A follow-up should be conducted post audit to ensure the completion of the recommended actions. Any inconsistencies noted or any delays in the completion of the recommended actions should be documented. Notwithstanding the risk-based approach, a comprehensive independent audit should be completed every two (2) years.

11. **AMENDMENT OF SCHEDULE - PARAGRAPH 34**.

The Schedule to the Regulations is amended in paragraph 34 by replacing it as follows

" 34. **Conducting a Customer Risk Assessment.**

(1) A customer risk assessment must be conducted on all new and existing customers. Prior to the establishment of a business relationship with the applicant for business and periodically thereafter, the regulated business shall assess the risk or otherwise of the applicant for business, the required financial services product and any other relevant factors. Based on this assessment, the regulated business must decide whether or not to accept the business relationship or to continue with it.

(2) In the case of existing customers, a risk assessment should be conducted in the following cases where

(a) a risk assessment was not conducted prior to establishing a business relationship and the customer remains a customer;

(b) there has been a change in the customer's behaviour or transactions;

(c) there has been a change in the customer's information since the commencement of the business relationship.

(3) The regulated business should take the following steps when conducting a customer risk assessment:

(a) identify the customer type including:

(i) individuals, whether domestic or international;

(ii) corporation or company whether domestic or international;

(iii) partnership;

(iv) trust;

(v) commercial bank, including correspondent banks;

(vi) money service businesses;

(vii) cash intensive businesses such as casinos and other gaming entities;

(viii) virtual asset service providers;

(ix) non-bank financial institutions; and

(x) politically exposed persons.

(b) collect the identification documents such as a Government-issued ID and proof of address verification documents. These documents should be used to obtain basic information as outlined in Paragraph 76. The appropriate identification and verification documents to be collected are listed in Paragraphs 77 – 84.

(c) conducting customer due diligence. When conducting customer due diligence, the following factors should be considered:

(i) turnover;

(ii) geographical origin of verification subjects;

(iii) geographical sphere of the verification subjects' activities;

(iv) nature of activity-frequency of activity;

(v) type and complexity of account or business relationship;

(vi) value of account/business relationship;

(vii) customer type;

(viii) customer behaviour;

(ix) the types of products and services being offered to the customer;

(x) the manner in which customers are introduced to the business;

(xi) a customer who has been introduced to the business (the person who introduced the customer to the business may not have carried out thorough 'due diligence' on the customer);

(xii) customers who are not local to the business;

(xiii) customers involved in a business that handles large amounts of cash;

(xiv) new customers carrying out large, one-off transactions;

(xv) the delivery channels and payment processes, for example cash over the counter, cheques, electronic transfers, virtual or digital currency or wire transfers;

(xvi) where customers' funds originate from or are transmitted to;

(xvii) whether "hold mail" arrangements are in place;

(xviii) whether an account or business relationship is dormant;

(xix) business with a complicated ownership structure that could conceal underlying beneficiaries;

(xx) a customer or group of customers makes regular transactions with the same individual or group of individuals;

(xxi) whether there is a form of delegated authority in place (eg. power of attorney, mixed boards and representative offices);

(xxii) a company issuing bearer shares or investments;

(xxiii) cash withdrawals or placement activity in or outside the jurisdiction;

(xxiv) suspicion or knowledge of money laundering or other crimes including the financing of terrorist activities.

(d) due diligence or investigative software and search engines via the World Wide Web may be used to verify whether a customer is on a Watch List or a Sanctions List.

12. **AMENDMENT OF SCHEDULE - PARAGRAPH 44.**

The Schedule to the Regulations is amended in paragraph 44 of the Guidance Notes in the Schedule as follows by:

(a) replacing the expression, "applicable to non-quoted corporate applicants (see paragraph 47 below)" with the expression, "**in accordance with the principles set out in paragraph 47**";

(b) inserting immediately after the expression, "general partner", the expression, "**as well as limited partners**"; and

(c) deleting the expression, "**Limited partners need not be verified**.".

13. **AMENDMENT OF SCHEDULE - PARAGRAPH 76.**

The Schedule to the Regulations is amended in paragraph 76 by replacing in the fourth bullet point, the expression, "current permanent address, including post code (any address printed on a personal account cheque tendered to open the account, if provided, should be compared with this address)" with the following**:**

- **" current permanent address, including postal code. This should be verified by one of the following documents listed below. The documents should not exceed the valid period specified at the time of establishing the business relationship or any time during an existing business relationship**

Proof of Address	**Valid Period**	**Proof of Address**	**Valid Period**
Utility Bill	3 months	Lease Agreement	Current
Bank Statement	3 months	Rental Property Contract	Current
Hire Purchase Statement	3 months	Property Insurance Policy	Current"
Letter from University/School	3 months		
Job Letter	3 months		
Inland Revenue Property Tax Receipt	6 months		

14. **AMENDMENT OF SCHEDULE - PARAGRAPH 99.**

The Regulations are amended in paragraph 99 subparagraph (g), by deleting the word, "significant".

15. **AMENDMENT OF SCHEDULE - PARAGRAPHS 122 AND 123.**

The Regulations are amended in paragraphs 122 and 123 by replacing them with the following:

" **122. WIRE TRANSFERS**

(a) Wire transfers have been identified as particularly vulnerable to being used for terrorist financing and money laundering. "Wire transfer and funds transfer" refer to any transaction carried out on behalf of an originator person (both natural and legal) through a financial institution by electronic means with a view to making an amount of money available to a beneficiary person at another financial institution. The originator and the beneficiary may be the same person. The originator is the account holder, or where there is no account, the person (natural or legal) that places the order with the financial institution to perform the wire transfer.

(b) Wire transfers can be cross-border or domestic. Cross-border transfer means any wire transfer where the originator and beneficiary institutions are located in different jurisdictions. This term also refers to any chain of wire transfers that has at least one cross-border element. Domestic transfer means any wire transfer where the originator and beneficiary institutions are located in the same jurisdiction. This term therefore refers to any chain of wire transfers that takes places entirely within the borders of a single jurisdiction, even though the system used to effect the wire transfer may be located in another jurisdiction.

(c) Financial institutions shall take measures to include full originator information, that is, accurate and meaningful originator information being the name, address and account number and beneficiary information on funds transfers and related messages that are sent, and the information shall remain with the transfer or related message though the payment chain. Financial institutions shall conduct enhanced scrutiny of and monitor for suspicious activity, funds transfers which do not contain complete originator information and beneficiary information. However, where there is a suspicion of money laundering or terrorist financing, the financial institution shall verify the information pertaining to its customer.

123. CROSS-BORDER WIRE TRANSFERS

(a) Cross-border wire transfers shall be accompanied by accurate and meaningful originator information that must, at a minimum, include the name and address of the originator and an account. In the absence of an account, a unique reference number must be included. However, the financial institutions may, in their discretion, substitute the address with a national identity number, customer identification number or date and place of birth. The accuracy of all information collected must also be verified.

(b) Information must also be obtained on the beneficiary of the wire transfer and shall include:

(a) the name of the beneficiary; and

(b) the beneficiary account number where an account is used to process the transaction; or in the absence of an account, a unique transaction reference number which permits traceability of the transaction.

(c) Where several individual transfers from a single originator are bundled in a batch file for transaction to beneficiaries in another country, they shall be exempted from including full originator information, provided that they include the originator's account number or unique reference number, and that the batch file contains full originator information that is fully traceable within the recipient country. However, financial institutions shall ensure that non-routine transactions are not batched since this would increase the risk of money laundering or terrorist financing.

123A. DOMESTIC WIRE TRANSFERS

Information accompanying domestic wire transfers must also include the same originator information as indicated for cross-border wire transfers, unless the bank is satisfied that the full originator information can be made available to the beneficiary financial institution and appropriate authorities by other means. In this latter case, the financial institution need only include the account number identifier provided that this number or identifier will permit the transaction to be traced back to the originator or the beneficiary. The information must be made available by the ordering financial institution within three (3) business days of receiving the request either from the beneficiary financial institution or from appropriate authorities.

123B. EXEMPTIONS

The above guidelines regarding wire transfers do not cover any transfers that flow from a transaction carried out using a credit or debit card so long as the credit card or debit card number accompanies all transfers flowing from the transaction. They also do not apply to financial institution-to-financial institution transfers and settlements where both the originator and beneficiary are financial institutions acting on their own behalf. However, when credit or debit cards are used as a payment system to effect a money transfer, they are covered by these guidelines, and the necessary information shall be included in the message.

123C. ROLE OF ORDERING FINANCIAL INSTITUTIONS

(1) The ordering financial institution shall ensure that:

(a) qualifying wire transfers contain complete originator information, which must be verified for accuracy.

(b) a wire transfer contains required beneficiary information.

(2) The ordering financial institution shall maintain all originator and beneficiary information collected in accordance with record keeping requirements of the relevant laws.

(3) The ordering financial institution shall not execute a wire transfer that does not comply with the requirements in this section.

123D. ROLE OF INTERMEDIARY FINANCIAL INSTITUTIONS

(a) For both cross-border and domestic wire transfers, financial institutions processing an intermediary element of such chains of wire transfers must ensure that all originator information that accompanies a wire transfer is retained with the transfer.

(b) Where technical limitations prevent the required originator or beneficiary information accompanying a cross-border wire transfer from remaining with a related domestic wire transfer, the intermediary financial institution must keep a record, for the minimum period under the relevant laws, of all the information received from the ordering financial institution or another intermediary financial institution.

(c) Intermediary financial institutions shall take reasonable measures, consistent with straight-through processing, to identify cross-border transfers that lack required originator information or required beneficiary information.

(d) Intermediary financial institutions shall have risk–based policies and procedures for determining (a) when to execute, reject or suspend a wire transfer lacking required originator or required beneficiary information; and (b) the appropriate follow up action.

123E ROLE OF BENEFICIARY FINANCIAL INSTITUTIONS

(a) Beneficiary financial institutions are required to have effective risk-based procedures for identifying and handling wire transfers that are not accompanied by complete originator information. The lack of such information may be considered as a factor in assessing whether wire transfers or related transactions are suspicious and, as appropriate, whether they are thus required to be reported to the Financial Intelligence Unit. In addition, beneficiary financial institutions must consider restricting or even terminating their business relationships with financial institutions that fail to maintain proper originator information.

(b) Beneficiary financial institutions are required to take reasonable measures,which may include post-event monitoring or real-time monitoring where feasible, to identify cross-border wire transfers that lack required originator information or required beneficiary information.

(c) For cross-border wire transfers, a beneficiary financial institution shall verify the identity of the beneficiary, if the identity has not been previously identified, and maintain a record of that information in accordance with the record keeping requirements of the relevant laws.

(d) Beneficiary financial institutions shall have risk-based policies and procedures for determining

(i) when to execute, reject or suspend a wire transfer lacking required originator or required beneficiary information; and

(ii) the appropriate follow up action.

(e) Financial institutions shall take freezing action and comply with prohibitions from conducting transactions with designated persons and entities, as per obligations set out in the relevant UNSCR relating to the prevention and suppression of terrorism and terrorist financing, such as UNSCRs 1267 and 1373 and their successor resolutions.".

16. AMENDMENT OF SCHEDULE - PARAGRAPH 131.

The Schedule to the Regulations is amended in paragraph 131 by replacing the heading, "Training", with the expression, "**Training, Recruitment and Employee Screening".**

17. AMENDMENT OF SCHEDULE - PARAGRAPH 133

The Schedule to the Regulations is amended in paragraph 133 by

(a) replacing the heading, "Training Programmes", with the expression, "**Training Programmes and Know Your Employee Procedures";**

(b) inserting immediately after paragraph b, the following new paragraphs

" **c.** A regulated business should obtain relevant, complete background information on each employee. The following information should be collected prior to the completion of the recruitment process and acceptance of a new employee

(i) the full name, permanent residential address, and contact numbers of the potential employee;

(ii) copies of identification documents and proof of address verification documents to verify the information collected pursuant to subparagraph (i);

(iii) any criminal record;

(iv) how well the potential employee performed at his or her previous organization;

(v) character references and professional references of the potential employee which should be requested by the employer if not provided;

(vi) the credentials, past experience, specialisation and interest levels of their potential employees including a résumé outlining the employment experience, educational history and skills;

(vii) how frequently he or she has changed employment with other organizations.

d. Where documents are requested or provided pursuant to paragraph (c), the originals of these documents should be reviewed and certified copies taken, where necessary. Reference checks should be conducted to verify the authenticity of an individual.

e. ***Monitoring Employee Behaviour***

Management should monitor employees' behaviour to identify any situation which might be considered suspicious. The following are some examples of suspicious conduct:

(i) lifestyle and spending habits which are not consistent with their salary, financial position or level of indebtedness;

(ii) sudden and significant changes in their standard of living;

(iii) if an employee refuses to take vacation for no apparent reason;

(iv) employees who do not allow other colleagues to assist certain customers;

(v) if an employee suspiciously receives gifts or gratuities on a regular basis;

(vi) employees who are reluctant to accept any promotions or changes in their activities; and

(vii) employees who stay at the office after working hours or that go to the office at odd times for no reasonable explanation.

(f) Management should also assess if an employee is performing his or her duties effectively and efficiently or whether additional training is required for improvement. It is essential that Management conducts regular employee evaluations to determine whether an employee is performing his or her duties in accordance with various company policies and procedures as well as regulatory requirements. Employee evaluations can also assist in revealing threats to a business.

(g) ***Human Resources Files***

Human Resources Files should be maintained for all employees containing the following:

(i) basic information on an employee such as name, address and emergency contact information;

(ii) a résumé;

(iii) an employment letter or contract, as well as the job description;

(iv) certified copies of qualifications earned;

(v) at least two reference letters;

(vi) copies of training certificates;

(vii) a police record;

(viii) performance evaluations or appraisals;

(ix) records of vacation;

(x) any disciplinary actions taken against the employee; and

(xi) any due diligence or background checks performed on the employee;

(h) Management should conduct regular reviews of employees' human resource files referred to in paragraph (g) and consequently should ensure that any necessary updates are made to those files to reflect such changes as revised job descriptions, copies of new qualifications earned, copies of certificates representing training received and periodic performance evaluations or appraisals, as necessary.

18. **AMENDMENT OF SCHEDULE - PARAGRAPH 173**.

The Schedule is amended by replacing the first bullet point in paragraph 173 with the following:

" The trustees, settlors, beneficiaries and protectors (if any) shall be treated as verification subjects where a settlement is to be made, when accepting trusteeship from a previous trustee or when there are changes to the trustees, settlors, beneficiaries or protectors.".

19. **AMENDMENT OF SCHEDULE - PARAGRAPH 178**.

The Schedule is amended in paragraph 178, by replacing the expression, "should" with the expression, "shall".

20. **AMENDMENT OF SCHEDULE**.

The Schedule is amended as follows:

(a) by inserting immediately after paragraph 183, the following new paragraph

" 183A. **LIFE INSURANCE BUSINESS.**

Life insurance business in relation to identification of the beneficiary under the policy.

(a) In relation to life insurance business, identification and verification should take place as soon as the beneficiary is identified or designated, and in all cases at or before the payout or the time when the beneficiary intends to exercise vested rights under the policy.

(b) In relation to life insurance policies, regulated businesses should take reasonable measures to determine whether the beneficiaries and, where required, the beneficial owner of the beneficiary, are politically exposed persons. This should occur, at the latest, at the time of the payout. Where higher risks are identified, regulated businesses should be required to inform senior management before the payout of the policy proceeds, to conduct enhanced scrutiny on the whole business relationship with the policyholder, and to consider making a suspicious transaction report.

(c) Regulated businesses should include the beneficiary of a life insurance policy as a relevant risk factor in determining whether enhanced customer due diligence measures are applicable. If a beneficiary who

is a legal person or legal arrangement presents a higher risk, enhanced measures should be taken, including reasonable measures to identify and verify the identity of the beneficial owner of the beneficiary, at the time of the payout.

(b) in Part VI, under the heading, Politically Exposed Persons (PEP) Risk, by inserting in paragraph 2 thereof, immediately after the expression, "and close associates.", the following new sentence:

" this category includes individuals who are or who have been entrusted domestically with prominent public functions including Heads of State or of Government, senior politicians, senior government, judicial or military officials, senior executives of state-owned corporations, and important political party officials.".

Made this 28th day of August, 2020.

TIMOTHY HARRIS
Minister responsible for Finance

GOVERNMENT PRINTERY
ST KITTS W I