SVG Financial Services Authority

Newsletter

ISSUE No.2: June 2025

Anchored in stability. Driven by Awareness. Trusted by the Public.

Welcome to Our Second Edition

We are pleased to present the second issue of our newsletter, continuing our commitment to keeping you informed about critical developments within the FSA and St. Vincent and the Grenadines' financial services landscape.

As the Financial Services Authority, we remain dedicated to maintaining the integrity and stability of our financial system while ensuring compliance with international standards. This edition reflects our ongoing efforts to provide accurate, timely, and proactive information that supports both regulatory compliance and industry growth.

Inside this issue

VIRTUAL ASSET SUPERVISION IN ST. VINCENT AND THE GRENADINES

St. Vincent and the Grenadines (SVG) has sought to adapt to the ever-evolving global financial market and has introduced a robust set of laws and regulations for virtual asset service providers (VASP).

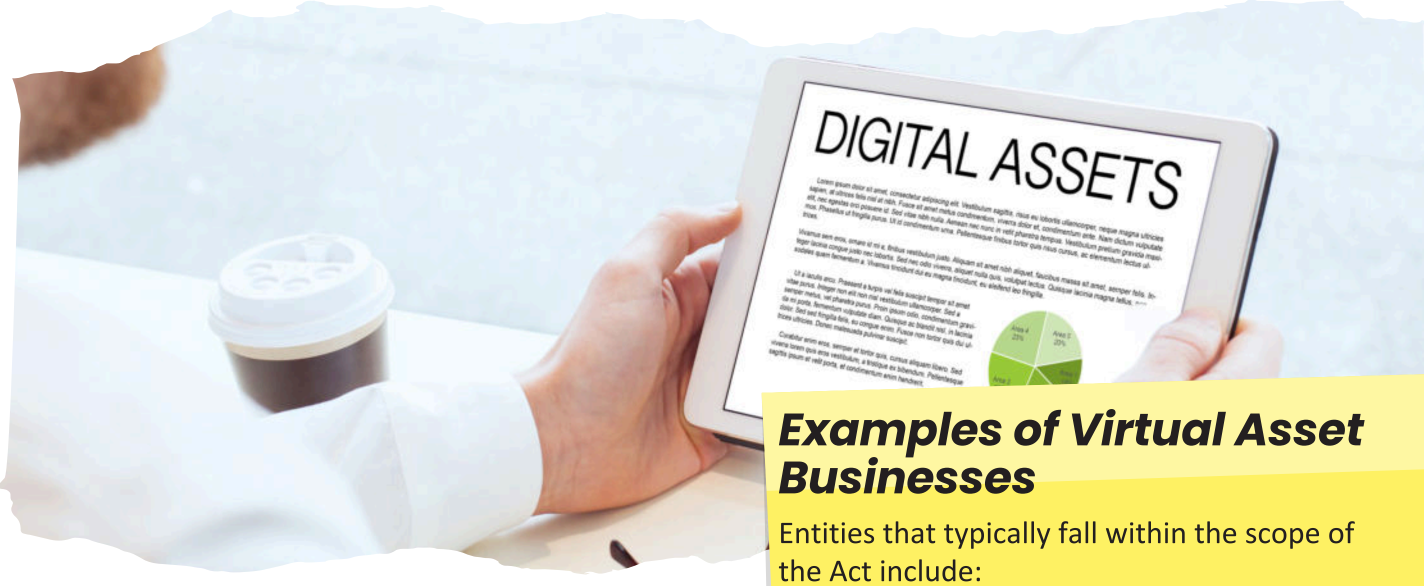
Virtual Assets: A Brief Overview

Virtual assets are items of value that are represented digitally, are recorded on a cryptographically secured distributed ledger, and are not fiat currency (which is issued by the government). Virtual assets can include:

- Stable coins
- Convertible virtual currency
- Non-fungible tokens (NFTs)
- Cryptocurrency

These types of assets are used to make payments or investments. They can also be transferred or traded. Virtual Asset Service Providers which operate in or from within SVG will be required to be registered under the Act.

Karen Jackson, Manager - IFS Department.



What is a Virtual Asset Business (VAB)?

The Financial Services Authority (FSA) reminds stakeholders that under the Virtual Asset Business Act (VABA), a Virtual Asset Business (VAB) refers to certain activities involving virtual assets when conducted on behalf of another person. These activities include:

- Exchanging virtual assets and fiat currency
- Exchanging one or more forms of virtual assets
- Transferring virtual assets, whether or not for value
- Safekeeping or administering virtual assets or related instruments
- Providing financial services related to the issuance or sale of virtual assets

Examples of Virtual Asset Businesses

Entities that typically fall within the scope of the Act include:

- Crypto Exchanges – Platforms that facilitate trading between virtual assets and fiat or other crypto assets (e.g. BTC/ETH spot trading)
- Crypto Transfer Services – Businesses that send or receive cryptocurrencies for clients
- Crypto Wallet Providers – Platforms offering hosted wallets and holding users' private keys
- Cryptocurrency Issuers – Companies issuing tokens, stablecoins, or NFTs for public use
- Crypto Payment Processors – Services enabling merchants to accept crypto payment
- Crypto Custodians – Entities securely storing virtual assets on behalf of clients
- Crypto Payroll Providers – Companies that facilitate payment of wages in cryptocurrencies

What is Not Considered a VAB

Some activities are not classified as VAB under the Act. These include:

✕ A company solely offering technology infrastructure (e.g. cloud storage)

✕ A private individual making a one-time crypto transfer

✕ A business using cryptocurrency exclusively for its own transactions

Entities or platforms that do not control customer funds or private keys (such as non-custodial wallets or fully decentralized applications) are generally outside the scope of the Act, but may still be subject to regulatory review on a case-by-case basis.

Examples of Virtual Assets

- Cryptocurrencies (e.g. Bitcoin, Ethereum, Solana)
- Stablecoins (e.g. USDT, pegged to fiat)
- Certain Non-Fungible Tokens (NFTs), when used as payment or investment tools

What Are Not Virtual Assets

- Fiat currency (e.g. USD, ECD) in bank accounts
- Traditional securities (e.g. stocks, bonds)
- NFTs that function solely as collectibles

For more information, or to determine whether your business activities may qualify as a VAB, please contact the FSA or refer to the full text of the Virtual Asset Business Act.

VIRTUAL ASSET BUSINESS (AMENDMENT) ACT, 2025

On April 28th, 2025 the Virtual Asset Business Act was amended to update and clarify certain provisions of the VABA. The key amendments are as follows:

- **Commencement date** -

The Amendment Act sets out the date for the commencement of the Act and makes it clear that the Act comes into force on the 31st day of May, 2025.

- **Proof of Incorporation (Section 6(3)(d))**

The amendment clarifies that applicants for registration must provide proof of incorporation or formation under either the Business Companies (Amendment and Consolidation) Act, or the Limited Liability Companies Act.

- **Regulatory Compliance References (Sections 18(1)(a) & 19(1)(d))**

The language is expanded to include not just the Act, but also Regulations made under it, ensuring that regulatory obligations apply broadly across both the Act and any subordinate legislation.

- **Extension of transitional Period (Section 24(2))**

The transitional period for the making of applications for registration for VASPs which were in operation prior to the commencement of the Act is extended from seven (7) days to thirty (30) days, providing more flexibility for compliance.

Anti Money Laundering/Terrorist Financing (AML/TF) Requirements for Virtual Asset Business

Virtual Asset Businesses (VABs) operate in a sector that is inherently vulnerable to money laundering (ML) and terrorist financing (TF) risks. These risks are primarily driven by the decentralized, pseudonymous and cross-border nature of virtual assets.

Virtual assets allow for the instantaneous transfer of value across jurisdictions without the involvement of traditional financial intermediaries. These characteristics present unique challenges for regulatory oversight and law enforcement. Thus, it is imperative that all VABs implement robust AML/CFT frameworks tailored to the specific risks of their business model and customer base.

Here are some recommended risk mitigation measures:

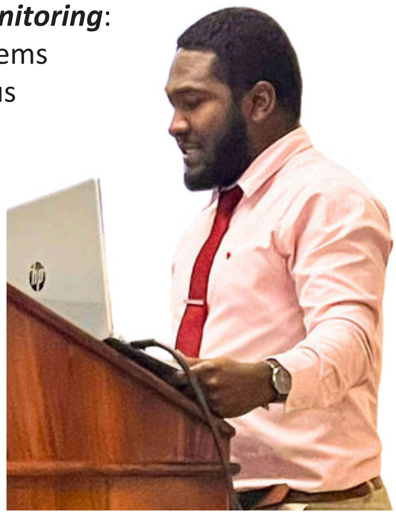
1. ***Know Your Customer (KYC)***:
   Conduct thorough onboarding and identity verification of all clients

2. ***Customer Due Diligence (CDD***):
   Continuously assess and monitor client behavior and risk levels

3. ***Enhanced Due Diligence (EDD):***
   Apply appropriate measures where higher risk indicators are present- such as customers from high-risk jurisdictions, complex ownership structures.

4. ***Transaction Monitoring***:
   Implement systems to flag suspicious transaction and patterns

5. ***Reporting Obligations***:
   Promptly report suspicious activity to the relevant authority (FIU)



Kalique Peters, Examiner - IFS Dept.

6. ***Ongoing Training***:
   Equip staff with training on evolving virtual asset risks and red flags

7. ***Risk-Based Approach***:
   Tailor controls according to the product type, customer risk, and geographic exposure.

As the virtual asset landscape continues to evolve, so too must the risk management and compliance culture of VABs. The ability to proactively detect and mitigate ML/TF risks is not only a regulatory requirement but a critical factor in ensuring long-term business sustainability and public trust.

Understanding Underinsurance

Your home is typically your most valuable asset, therefore the last thing you want to hear when you file a claim with your insurer for damage to your home, is that the insurer won't cover your total loss or that your insurer is refusing to pay the full value of your claim.

But that can be one of the very real and unfortunate consequences of underinsurance. While some people are unaware that they are underinsured, many don't think about it until it's too late.

What is underinsurance?

Underinsurance refers to a situation where the insurance coverage that you have in place is insufficient to cover the full value of the loss or damages incurred.

Signs you may be underinsured

Being adequately insured doesn't end with getting insurance coverage as a 'set and forget'. It is important to remember that your circumstances will change over time, and as a result, your insurance needs will too. Not reviewing your policies when they are up for renewal or proactively when your circumstances change can leave you vulnerable- a risk faced by many.

Here are some signs that you may be underinsured:

1. Outdated Policy- If your policy has not been reviewed or updated in several years, it may not reflect the building or content's current value.
2. Modifications and improvements- Renovations and upgrades to the building can affect the value of your property and ultimately your insurance coverage. You could be left underinsured if your insurance policy is not updated to reflect these changes.
3. Inflation- Rising property values and construction costs may mean you are not fully protected.
4. High-value Items- If you buy expensive items like electronics or furniture and do not add them to your policy, you could be left underinsured
5. Underestimated Rebuilding Costs- If the initial estimation of a rebuild cost was too low, your coverage might not be enough to cover a complete rebuild.

What are the consequences of underinsurance?

Being underinsured can have serious consequences. If a fire, flood or other disaster affects your property and you need to make a claim, the gap between your coverage and the actual loss can be significant. It is therefore, your responsibility to ensure that you are insured for the full replacement value or rebuild cost. Failure to do so can have inconvenient and costly consequences such as:

1. Receiving a reduced payout

The most obvious consequence is that the payout you receive from your claim will not be as high as anticipated. Insurance policies often include an 'average clause', which means that the insurer can reduce the payout in proportion to the underinsurance. For example, if your property is insured for half of its actual value, the insurer might only cover half of your claim.

2. Possible voiding of your policy

In the event that you are underinsured and you need to make a claim, your insurer may 'void' the policy, that is, cancel the policy altogether, by refunding all premiums paid.

3. Increased out-of-pocket costs

If your insurance payout is lower than what you expected due to being underinsured, you will need to cover the difference between the insurance payout and the actual cost of repairs or replacement. This can result in significant out of pocket expense.

How to avoid being underinsured

Avoiding underinsurance is crucial to ensure you're fully protected in the event of a loss. How do you ensure that you have the right amount of insurance for your property?

1. Get a Professional Valuation
Have your home or building professionally valued to determine its accurate replacement cost (not market value). That is the total cost to rebuild your property from scratch, including materials, labour and other associated expenses. Unlike the market value, the rebuild cost focuses on the actual expenses of reconstruction.
For contents, make a detailed inventory of each item and its worth, especially valuable items such as appliances, electronics, furniture and jewelry.

This helps to ensure your building and contents insurance will cover everything if you have a loss.

2. Insure for the Full Replacement Cost
Before providing you with a quote, your insurer will want to know the cost of replacing the contents of your property or business and/or the cost of rebuilding the property. Choose a coverage that reflects the cost to rebuild or replace your property, not just what you paid or owe.

3. Update Your Policy Regularly
Keep track of any improvements or modifications. When any changes are made to the building, the insurance policy needs to be updated. Additionally, construction and material costs can increase over time, making it difficult to keep insurance coverage aligned with current replacement costs.

Notifying your insurer of these changes and adjusting your policy to reflect current costs ensures your coverage remains adequate.

4. Be Honest and Accurate
Under-declaring the value of your property to obtain a lower premium can void claims. Provide full details when applying for insurance coverage. Omitting or misstating facts may lead to partial or denied payouts.

5. Consider Professional Advice
Seek guidance from a qualified and licensed insurance advisor to determine the appropriate coverage for your needs.
Remember, your home is your biggest asset, therefore, you must ensure that it is adequately insured.

Effective Board Oversight (AML/CFT/CPF)

The Board of Directors ("the Board") of a service provider has ultimate responsibility for the effectiveness of its AML/CFT/CPF programme.

Therefore, knowledge of the jurisdiction's legal requirements for money laundering, terrorist financing and proliferation financing (ML/TF/PF) is critical for them to execute their duties effectively.

In its role, the Board must align corporate objectives with regulatory expectations to design and implement a risk-based AML/CFT/CPF compliance program. In St. Vincent and the Grenadines, the effectiveness of this programme is evaluated against a Five Pillar Approach to AML/CFT Governance, which assesses the Risk Management Framework, Compliance Function, Internal Controls, Training Programme and Independent Testing, adopted by service providers.

These five pillars provide a broad-based and dynamic approach to AML/CFT/CPF compliance monitoring and management activities. By utilizing the five-pillar approach for compliance, service providers are supporting the jurisdiction's efforts to ensure that ethical and responsible financial practices are enforced to detect, prevent, and report financial crimes.

Let's now examine how each pillar aids effective oversight.

Risk Management Framework

A credible risk management framework must be supported by appropriate governance arrangements and commitments. The Board must centralize the compliance programme around a risk-based approach, i.e. establish a framework that enables risks to be identified, assessed, and managed.

This would include:

- formulating and documenting the risk appetite statement and risk tolerance levels for the institution
- developing the risk assessment methodology,
- designing and implementing policies, procedures and systems that are commensurate with the identified risk.
- employing suitably skilled professionals to manage the programme.
- ensuring the compliance function has adequate resources to operationalise the programme.

These actions will support AML/CFT/CPF risk management and enable the Board to exercise reasonable judgment and oversight of financial crime risk.

Compliance Function

The compliance function is another critical element of an effective AML/CFT/CPF regime.

The compliance officer is appointed by the board to operationalise and oversee the day-to-day activities. Compliance officers ensure that the compliance approach is seamlessly integrated into the service provider's processes.

Their roles and responsibilities include monitoring and managing the business compliance with the local laws and international best practices, updating policies and procedures, and reporting suspicious activities. They are the second line of defense in the AML/CFT/CPF regime.

Internal Controls (AML/CFT/CPF)

To prevent the entity from being used by criminals, the Board must ensure that the controls supporting its AML/CFT/CPF regime are adequately designed, functional, and dynamic.

The effectiveness of these controls must be monitored and managed. Monitoring must be an ongoing, seamless process where the system's capability to detect and mitigate against ML/TF/PF is systematically evaluated, and identified gaps are acknowledged and managed.

The internal and external audit functions play a crucial role in the effectiveness of this pillar. This is because they evaluate the veracity of the system against the legislative requirements, and established policies and procedures.

A timely and reciprocal reporting mechanism, proportionate accountability measures, prompt corrective action, and relevant staff training must support the element of internal controls.

Training

An effective training programme within a service provider's AML/CFT/CPF regime should include periodic and appropriate training for all relevant roles. Effective training should have general components such as building legislative awareness and knowledge. However, certain aspects, particularly relating to the controls and the roles and responsibilities of employees within the overarching programme, must be tailored to improve the effectiveness of the system.

An effective training programme will include regular and refresher training for the Board and management, and be designed to facilitate ad hoc sessions to inform relevant persons of significant legislative amendments, system changes, and to implement recommendations from internal or external assessments.

Independent Testing

This element of effective board oversight focuses on testing controls and evaluating the interaction between people, systems, and processes to ensure an effective interface and that mitigation strategies are efficient.

The Board's duty under this pillar is not to execute the assessment, but to ensure that these reviews are embedded within the framework and are performed as prescribed.

Further guidance is outlined in the Anti-money Laundering and Terrorist Financing Code, 2017, Paragraph 24 and its accompanying Guidance Notes.

Building Financial Literacy Across St. Vincent and the Grenadines

As part of its strategic initiative to increase public awareness and improve financial literacy in St. Vincent and the Grenadines, the FSA participated in two (2) Business Development Workshops hosted by the Adult and Continuing Education Division within the Ministry of Education. The FSA presented on several topics including pyramid schemes, importance of property insurance and consumer protection in micro-financing.

Financial Services Authority staff members at the Argyle RC Primary School. Left to right: Nyasha Browne, Manager of Credit Union Department; Sashaw Dublin, Examiner in the Credit Union Department; Mintrue Rose-Providence, Manager of Insurance and Pensions; and Laffa Francois, Examiner in the Insurance and Pensions Department, with a participant delivering the vote of thanks.

Financial Services Authority executives at the Layou Learning Resource Centre. Left to right: Deputy Executive Director, Derek St.Rose and Executive Director Carla James.

Thank you for reading!

The FSA welcomes your feedback and suggestions towards improving the utility of this newsletter to your institution. Please make your submissions to:

Email: info@svgfsa.com

Click to Connect With Us

Financial Services Authority
St. Vincent and the Grenadines

Address

2nd Floor,
Inland Revenue Building
Grenville Street
P.O. Box 356, Kingstown
St. Vincent & the Grenadines

Website/Email

www.fsasvg.com

info@svgfsa.com

Phone

+1784-456-2577

+1 (784) 457 2328

+1 (784) 485 6031