



RAHN MONITOR

Your one-stop Sanctions, Adverse Media screening and reporting solution, designed to take your 'Know your customer' to the next level.

Crypto Service Providers

The FIC Act has expanded the scope of compliance to include Crypto Asset Providers to fall within the FIC's supervisory function. Under the act, this sector and its professions are called the designated non-financial businesses and professions (DNFBPs).

Crypto Asset Providers are now classified as accountable institutions, subjecting them to enhanced AML (Anti-Money Laundering), CFT (Counter Financing of Terrorism), and CPF (Counter Proliferation Financing) supervision by the Financial Intelligence Centre (FIC).

As a result, Crypto Asset Providers must adhere to stricter compliance standards and reporting obligations, ensuring greater transparency and regulatory oversight within these industries.

Crypto asset service provider Definition

Item 22: A person who carries on the business of one or more of the following activities or operations for or on behalf of a client:

- (a) Exchanging a crypto asset for a fiat currency or vice versa;
- (b) exchanging one form of crypto asset for another;
- (c) conducting a transaction that transfers a crypto asset from one crypto asset address or account to another;
- (d) safekeeping or administration of a crypto asset or an instrument enabling control over a crypto asset; and
- (e) participation in and provision of financial services related to an issuer's offer or sale of a crypto asset, where "crypto asset" means a digital representation of perceived value that can be traded or transferred electronically within a community of users of the internet who consider it as a medium of exchange, unit of account or store of value and use it for payment or investment purposes, but does not include a digital representation of a fiat currency or a security as defined in the Financial Markets Act, 2012 (Act 19 of 2012).

Public compliance communication

- [PCC 57](#)
- [PCC 53](#) – RMCPs

Recommendations

With the introduction of the amended Financial Intelligence Centre Act (FIC Act), certain obligations have been placed on Crypto Asset Providers to ensure they play a proactive role in the detection and prevention of money laundering and financing of terrorism.

These obligations are critical in maintaining the integrity of Crypto Asset Providers.

- Perform customer due diligence
- Report suspicious transactions
- Maintain comprehensive records
- Implement internal controls and compliance measures
- Conduct risk assessments
- Report cash threshold transactions.

The measures collectively aim to enhance the accountability of Crypto Asset Providers.

Other material

- [Directive 7](#)
- [Reference guide](#)



RAHN MONITOR

Your one-stop Sanctions, Adverse Media screening and reporting solution, designed to take your 'Know your customer' to the next level.

What is the FIC

The FIC Act introduces a regulatory framework of measures requiring certain categories of business to fulfil compliance obligations.

The FIC Act deems these categories of business, called accountable institutions, as being vulnerable to being abused by criminals for money laundering and terrorist financing purposes.

All FIC Act compliance obligations are premised on institutions implementing a risk-based approach to combating money laundering and terrorist financing. Refer to the [Reference guide for all accountable institutions](#) for more information on the FIC Act obligations.

The Public compliance communication (PCC) provides guidance on Targeted Financial Sanctions (TFS), and recommendations regarding the implementation of a risk-based approach to combatting proliferation financing (CPF) and activity-based sanctions.

The [PCC](#) also provides clarity on certain definitions including counterproliferation financing of weapons of mass destruction and sets out heightened risk scenarios.

Penalties for non-compliance can range from **R 10 000** up to **R 1 mil** fine for more severe violations such as failure to report suspicious transactions or inadequate customer due diligence.

FIC Act Requirements

- Register with the FIC
- Submit regulatory reports to the FIC
- Implement a risk-based approach
- Develop a risk management and compliance programme
- Determine beneficial ownership
- Conduct customer due diligence
- Determine if clients are politically exposed persons
- Monitor transactions
- Keep records of customer transactions
- Appoint a compliance officer
- Train employees on how to comply with the FIC Act

What the FIC does

- Receive regulatory reports and transaction and other data from accountable institutions and other business
- Interpret and analyse the data received
- Produce financial intelligence from this data for the use of competent authorities in their investigations, prosecutions and applications for asset forfeiture
- Produce forensic evidence based on the flow of financial transactions
- Exchange information with bodies that have similar objectives in other countries regarding combating of ML, TF and PF (money laundering, terrorist financing and proliferation financing), and other similar activities
- Facilitate effective supervision and enforcement by supervisory bodies



RAHN MONITOR

Your one-stop Sanctions, Adverse Media screening and reporting solution, designed to take your 'Know your customer' to the next level.



Updated Daily



Pay-as-you-go



API Availability

About Rahn Monitor

Explore our sophisticated platform called RAHN Monitor, designed to take KYC (know your customer) to the next level. Whether you are required to comply with Anti-Money Laundering legislation or simply need to ensure that you are only doing business with individuals and entities that are above board, we have you covered.

With built-in Artificial Intelligence (AI) capabilities that take the grunt work out of investigations to multiple integration points, it has never been simpler to ensure that you are in control of the risks within your customer base.

Multi-Phased Approach

1

Global Sanctions Coverage

Our dataset brings together the most prominent sanctions lists across the globe and is updated daily.

2

Advanced Match Algorithm

Our Advanced search algorithm incorporates multiple fuzzy logic options, which combined with our probability score, gives you the confidence to clear potential hits quickly and effectively.

3

Custom Database

The custom dataset functionality allows any company to build their own internal do-not-do-business list which can help ensure no unwanted elements are onboarded into the company.

Who is it for?

Rahn Monitor is a vital tool for Crypto Asset Providers who function as head compliance, ensuring adherence to regulations stipulated in the Financial Intelligence Centre Act (FIC Act).

It streamlines customer due diligence, suspicious transaction reporting, and record-keeping, helping to prevent money laundering and financing of terrorism.

With its user-friendly interface and robust features, Rahn Monitor simplifies compliance processes, reduces the risk of non-compliance, and helps avoid significant fines and reputational damage.

4

Adverse Media

The Adverse media function allows users to conduct this component of the client due diligence on individuals of interest.

5

Multiple Integration Points

Our system was designed for small, medium and large users by providing three different integration options.

6

Monitor-GPT

Our MonitorGPT AI assistant was designed to take Enhanced Due Diligence to the next level. We connected our AI to the internet and developed it to searches and creates a comprehensive overview for you.