EARLY WARNING AML TRANSACTION MONITORING

Better AML Risk Monitoring will reduce fraud and criminality while increasing compliance and security.

In response to increased terrorist attacks, governments have set their sights on bringing increased visibility to the money that leads to criminal and terrorist organisations with the likelihood of further regulation and more detailed compliance evidence in the future.

With the threat of enforcement actions, costly penalties and criminal charges against individuals, it is predicted that global spending on AML by financial services organisations could exceed $8 billion a year.

Given the need for risk mitigation across industries other than financial services, the figure is likely to be much higher -as is the need for organisations to implement effective due diligence processes to screen, monitor and protect against AML compliance failures.

The Problem:

BAFT (Bankers Association of Finance and Trade) estimates that 1% of the proceeds from financial crimes are intercepted. Meanwhile, nine out of ten suspicious activities flagged by AML transaction monitoring software in banks are false alarms. The natural conclusion is that the process models used by AML software are wrong most of the time which is increased work in filing unnecessary SARs (suspicious activity report) to be filed with FinCEN. In many cases, these false positives are due to the individual institution being unable to verify the bona fides of a person who is a client of another institution or even the same institution but in another jurisdiction.

New regulations are forcing all companies to obtain consent to share data with third parties, something impractical which users may not always agree to. The best approach, to ensure regulatory compliance, is to consider ways of gaining certainty over the transaction risk while not sharing a user's personal data in the process of quantifying that risk.

Can Technology Solve this Problem?

It is likely that regulation and oversight will bring even more pressure, and potentially greater shifts, in the way to governance, risk and compliance (GRC) programs need to operate to succeed. Technology that is used to power businesses is continually changing and improving and companies need to move away from constantly relying on humans to cover the gaps. People are an imperfect solution.

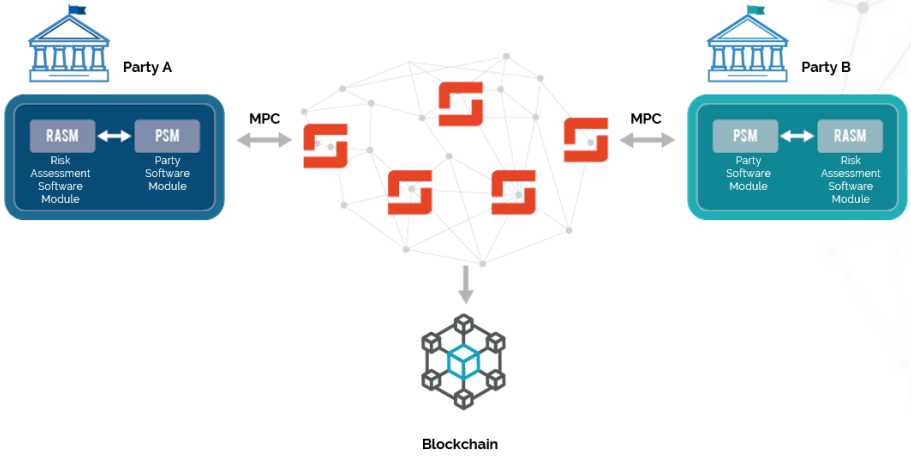
Authorities are at pains to emphasise the importance of using 'tools and systems' to identify, establish and monitor mandatory controls that should be inherent in the future. Using technology becomes even more essential when considering the main thrusts of the 5th AML Directive. Some of the key points being:

- **Transparency on beneficial ownership**
- **Wider access to beneficial ownership information**
- **Lowered thresholds for customer due diligence**
- **PEP lists**
- **Broader criteria for assessing country risk**
- **Enhanced due diligence in high-risk countries**
- **Improved information on customers**

Compliance versus data protection

We believe that increasing monitoring of transactions without violating client banking secrecy and other data protection regulations is a challenge that all companies complying with regulatory requirements as above have to address. As has been amply demonstrated, sending personal data, even when encrypted, is fraught with problems and in many instances does not comply with GDPR or other banking regulations.

The solution:



The solution is based on a specific type of MPC that only requires sending randomised data. No PII is ever exposed but the sending bank is able to learn whether a risk exists with the counterparty customer without the counterparty bank disclosing any information about their client. This addresses the problem of monitoring customer bank remittances for AML compliance without violating client banking secrecy and other data protection regulations.

The Value:

- **Increased regulatory compliance**
- **Reduction in false positives, increase in real positive alerts**
- **Real-time assessment of counterparty risk**
- **Reduction in need for RFI submissions**
- **Reduction / elimination of susceptibility to regulatory action / purposes**
- **Reduction / elimination of personal risks due to better risk identification**

Commercial Considerations:

The Sedicii solution can be deployed in an 'on premise' configuration where the client enterprise will manage and maintain the service entirely independently. In the 'on premise' configuration, it is sold on a licensed basis depending on the number of users and applications. Or, it can be provided in a cloud configuration where the same service may be shared by a number of organisations or services. In this configuration, the service is delivered on a transaction basis and managed entirely by Sedicii on behalf of the client enterprises.

Sedicii proves that a customer is not being impersonated, quickly, securely and reliably, WITHOUT any underlying sensitive personal information having to change hands. The attribute details of the online identity are NEVER exposed. This reduces the burden of responsibility on the financial institution while protecting the customer. All sides win.

See Sedicii in action…
We can set up a trial of our services. The implementation of the Sedicii server is done via the cloud or we can place a Sedicii server within your hosted environment.

Sedicii Headquarters, Ireland
ArcLabs Research & Innovation Centre,
WIT West Campus,
Carriganore,
Waterford. X91 P20H
Ireland

Sedicii Limited, UK
Techhub,
1-15 Clere St.,
London,
EC2A 4UY
UK

Phone: 353 51 302191 Email: contactus@sedicii.com Web: https://www.sedicii.com Twitter: @GBRSedicii