International Securities Services Association

Financial Crime Compliance

Bulletin December 2019

Mark Gem
ISSA Working Group co-Chair / Chief Compliance Officer Clearstream International

Olivier Goffard
ISSA Working Group co-Chair / Head of Compliance & Ethics Euroclear Group

Yannick Cherel
ISSA Working Group co-Chair / Group Product Head of Financial Crime Compliance, Standard Chartered Bank

Welcome to the December 2019 ISSA Financial Crime Compliance Bulletin.

In this edition, the Financial Crime Compliance Working Group will brief you on two topics which are currently of great interest to the securities services industry.

Sanctions Screening Best Practice

The monitoring of transactions in order to detect, prevent and disrupt financial crime is a key requirement for financial organizations. ISSA recently surveyed its members about the maturity of sanctions screening practices. The results of this survey form our new brief on the controls required in order to adopt best practice in effectively implementing the FCC Principles.

FCC Principles Update

We have already seen good traction in the market with the FCCP Due Diligence Questionnaire being increasingly integrated into custodians` due diligence practices. Tom Zeeb, SIX's Head of Securities & Exchanges, explains how SIX has implemented the FCC Principles.

Don't forget, January 2020 is the industry defined implementation date for the FCCPs.

The Financial Crime Compliance Working Group is headed by Clearstream's Mark Gem, Euroclear's Olivier Goffard and Standard Chartered's Yannick Cherel. They are supported by a team of industry experts from many of the world`s leading firms: BIL, BNP Paribas, BNY Mellon, Citigroup, Clearstream, Credit Suisse, Deutsche Bank, Deutsche Börse, DTCC, Euroclear, HSBC, RBC, SEB, SIX, Standard Chartered, SWIFT and UBS.

Sanctions Screening Best Practice

Introduction

ISSA has been at the forefront of the push to future-proof Financial Crime Compliance standards across the global securities services industry. Geopolitical developments have meant that international sanctions have become directly relevant to participants in the securities markets as policy makers deploy increasing complex sanctions` instruments.

Since - what is often referred to as – «the Russian Sanctions», lawmakers and regulators have made more frequent use of sanctions that have an impact on securities issued by sanctioned entities. The authorities see this as an effective way to detrimentally affect the economic situation of those entities. It is therefore anticipated that this approach is likely to be used increasingly in the future. Ensuring securities services providers have a robust sanctions screening mechanism in place is therefore paramount for the protection of the whole securities industry.

Principle 9 of the FCCPs states that omnibus accounts may only be opened if transactions passing through those accounts and account holdings are screened against the lists of designated persons under sanctions. Whilst a few years ago securities transactions were usually not screened for Financial Crime monitoring reasons, the landscape has evolved significantly and the screening of securities transactions against relevant sanctions watch lists – before the transaction is processed – has become the «gold standard» and is a control that should be standard across the securities services industry.

In this context, ISSA launched – in the summer of 2019 - a survey aimed at assessing how far this good practice was already embedded across ISSA participants.

Main Take-aways from the Survey

The survey covered the different angles of sanctions screening:

- Are securities transactions/instructions screened?
- Is the screening of additional information including tax, corporate actions, securities and share registration data also being covered?
- What is the frequency of the screening?
- Against which sanctions lists is the data screened (EU, US...)?

In summary, it was found that - although the vast majority of respondents (92%) confirmed that they screen securities transactions against EU and US watch lists - there were a number of discrepancies in how sanctions screening was taking place when the data was further reviewed.

Three key points which were noted show that:

- Whilst over two thirds of respondents screen transactions before they are processed, almost a third of the respondents do not - therefore exposing themselves and their counterparties to risk;
- Whilst the name of the Account Holder[1] is usually screened, there is still some room for improvement concerning the screening of other relevant sources of data such as information related to the Client of the Account Holder and/or Ultimate Assets Beneficial Owners' data as defined by the ISSA FCCPs. The Client of the Account Holder and/or Ultimate Assets Beneficial Owners' data is not screened by roughly one quarter of the surveyed population;
- With regards to other relevant sources of information; securities and issuers names, tax data and share registration data are also usually screened by 80% of the respondents. By screening these additional sources, key information can be included to improve detection and limit a sanction exposure.

5 Key Attention Points

ISSA intends to re-perform this survey in the course of 2020 to assess the evolution in the maturity of securities sanctions practices across the sector. However, in the interim, and in order to support securities services providers in improving their screening practices, we have issued the following 5 main attention points to support this exercise:

[1] Words with capital letters are those as defined in the FCC Principles

- **As well as screening cash instructions, all relevant securities message types should also be screened**
  Securities message types (settlement, corporate actions, income, tax…) that include structured or unstructured information, which might reveal a link with sanctioned parties should be screened. This includes - at a minimum - the name of the order giver and recipient of the transaction, BIC codes, any country information but also all free text fields which by definition could contain any type of information.

- **Direct client data, as well as intermediary and final beneficial owner data (where available), should be screened**
  With respect to client data, this concerns all data collected during the KYC exercise, including Entity Beneficial Owners' data (Board members, Shareholders…). In addition, should custodians be operating a final beneficial owner (BO) model, or with segregated account holders, it is important to ensure this information is screened as well.

- **Identify other relevant sources of information**
  More information on beneficial owners may be available down the chain than originally anticipated. Tax certificates holders, BOs collected in the context of disclosure requests or other corporate events…all contain names of individuals and companies that might reveal an exposure to sanctions risks. Those should be screened as well.

- **Screen the securities ecosystem**
  Issuers, issuing agent, paying agent… might be relevant information to screen as are securities names, ISINs/CUSIPs and prospectuses that might reveal links with sanctioned parties or countries.

- **Set up the screening so that it occurs «ex ante» and then on a daily basis**
  The regulatory expectation is that sanctions screening takes place on T-1, T being the time when a transaction is processed, a security is created in your system, a client is admitted etc. Also, if screening should be executed at the outset, information should also be screened on a daily basis to capture possible changes in your dynamic sources of information or in the sanctions watch list (which are usually updated daily).

FCC Principles Update

Thomas Zeeb
SIX

SIX

SIX's Head of Securities & Exchanges, Thomas Zeeb, explains how SIX has taken the ISSA Financial Crime Compliance Principles (FCCP) and implemented them within his organization.

«We committed early on to incorporate the FCC Principles into our due diligence process. As part of this exercise, SIX SIS AG implemented changes to its General Terms & Conditions which incorporate the disclosure conditions outlined in the FCC Principles as a condition of membership in the CSD. In addition, all of the elements contained within the FCCP Questionnaire have been incorporated into SIX's compulsory KYC and due diligence processes. More recently, these processes and the content required have been enshrined in a new IT-based Client Due Diligence and KYC process which allows for enhanced monitoring and follow-ups based on their respective risk profiles and market activities.»