Module Integrity of Financial Markets
by Vandana Doekhie, Senior Client Account Manager, BNP Paribas Asset Management

Welcome to the module Integrity of Financial Markets of the 2021 MiFID II Stay Compliant Program of CFA Society VBA Netherlands. Your presenter today is Vandana Doekhie, Senior Client Account Manager at BNP Paribas Asset Management.

Ethics and integrity matter

Ethics and integrity matter in daily life as well as in the financial sector. Dealing with other people's money brings a huge responsibility with regard to ethical behaviour and integrity. Ethics can be defined as a set of moral principles or rules of conduct that provide guidance for our behaviour when it affects others (definition CFA Institute). It relates to good and evil and right and wrong. Integrity refers to the quality of being honest and having strong moral principles (American dictionary).

CFA Society Netherlands | vba

Knowing the definition of ethical behaviour is not enough as we will see in the examples in the presentation. It is important to create a culture of integrity in the workplace. This concerns 1) Promoting ethical principles throughout the company; 2) the tone at top and 3) working in the best interest of clients.

This is important to promote a financial sector that is working to the ultimate benefit of society by having 1) trust of investors and 2) robust financial markets.

In this course, we will discuss some real life examples of integrity risks and the consequences of violations of duty. It is important to distinguish between integrity risks resulting from intentional threats like fraud or falsification, with the purpose of doing harm, versus integrity risks an organisation or individual person is exposed to due to neglect or vulnerability.

Furthermore, we will describe what companies, information providers and advisors need to pay attention to. Finally we will give examples of what you should and should not do in dealing with client integrity matters.

Case: ABN AMRO

The importance of ethics and integrity in the financial sector is regularly illustrated with real life examples that make the news. One example of insufficient controls concerns ABN AMRO. As early as 2014, a whistleblower reported information about dubious transactions. This eventually led to a large-scale DNB investigation, which included the domestic bank. After this however, ABN AMRO applied no fundamental approach to combat money laundering practices, and despite multiple DNB's findings, money laundering controls did not continue to function optimally. Even after ING Bank received a record fine of EUR 775 million in 2018 for similar transactions, ABN AMRO did not do enough to improve money laundering checks.

While the company eventually established a Financial Crime Detection department, controls remained inadequate. Several cases, such as a EUR 4.3 million fraud committed by a Royal FloraHolland employee via an ABN AMRO account and a EUR 23 million VAT fraud at a Rotterdam metal company came to light in this period. The Dutch Public Prosecution Service investigated the banks compliance with its obligations under the Dutch Anti-Money Laundering and Counter Terrorism Financing Act and confirmed a violation.

In April 2021, ABN AMRO settled with the Public Prosecution Service for a fine of EUR 480 million as a result of having insufficient money laundering controls in place. Not only the bank itself is dealing with consequences for this type of misconduct; it was also announced that three individual former executives are labelled as “suspects” in this settlement and their role in this case will be further investigated.

Integrity risks: examples

Recent history shows many examples where integrity risks materialise. From money laundering to tax evasion, conflicts of interest and cybercrime. Market abuse (MAR) is another well-known integrity risk, which includes activities such as market manipulation and insider dealing. The LIBOR scandal is one of the biggest known examples of market manipulation, whereby a number of banks conspired to manipulate the LIBOR rate, leading to enormous lawsuits, fines and regulatory actions. The Dutch market abuse regulations are based on European directives and regulations and laid down in the Dutch financial Supervision Act and the Market Abuse Decree.

The prevention of anti-money laundering (AML) and financing of terrorism is also a hot topic. The recent examples from ING and ABN AMRO showcase this. Examples like these make clear how difficult it is to build in proper AML procedures, including proper monitoring, reporting and adjustment procedures. Especially in international organizations with different cultures and (external) politics.

CFA Society Netherlands | vba

When events like these occur, they have a major impact on the trust people have in the financial sector. Therefore, authorities and regulators are more and more looking into this. These types of risks are not limited to large firms or to specific countries. Financial crime is global and will always take the path of least resistance. All financial market participants therefore need to familiarize themselves with both national and international laws and regulations on how to deal with violations in a proper way.

We will now highlight one type of integrity risks that is becoming more relevant every year: cybercrime.

Cybercrime

Digitalisation and technology are transforming the financial industry at a high speed and large scale. Robo-advice or semi-automatic investment management are new business models for financial institutions. The institutional sector has already progressed in this area, and private banks are rapidly following.

Regulators remain sceptical of such developments, given the increase in cybercrime the new technology could enable. Regulators are therefore increasing their focus on cyber security and are looking for assurances that businesses are taking the necessary steps to prevent breaches. Asset management firms and other financial institutions are attractive targets for cyberattacks and must institute appropriate preventative controls and monitoring procedures, as well as post-attack action plans.

The financial damage from this type of integrity risk is substantial: The Washington Post referred to a report from the Centre for Strategic and International studies and computer security company McAfee which projects the costs of cybercrime in the world almost reaching USD 1 trillion in 2020, and is expected to increase even further in the coming years. The worldwide move to work remotely due to Covid-19 has also contributed to this massive rise in cybercrime.

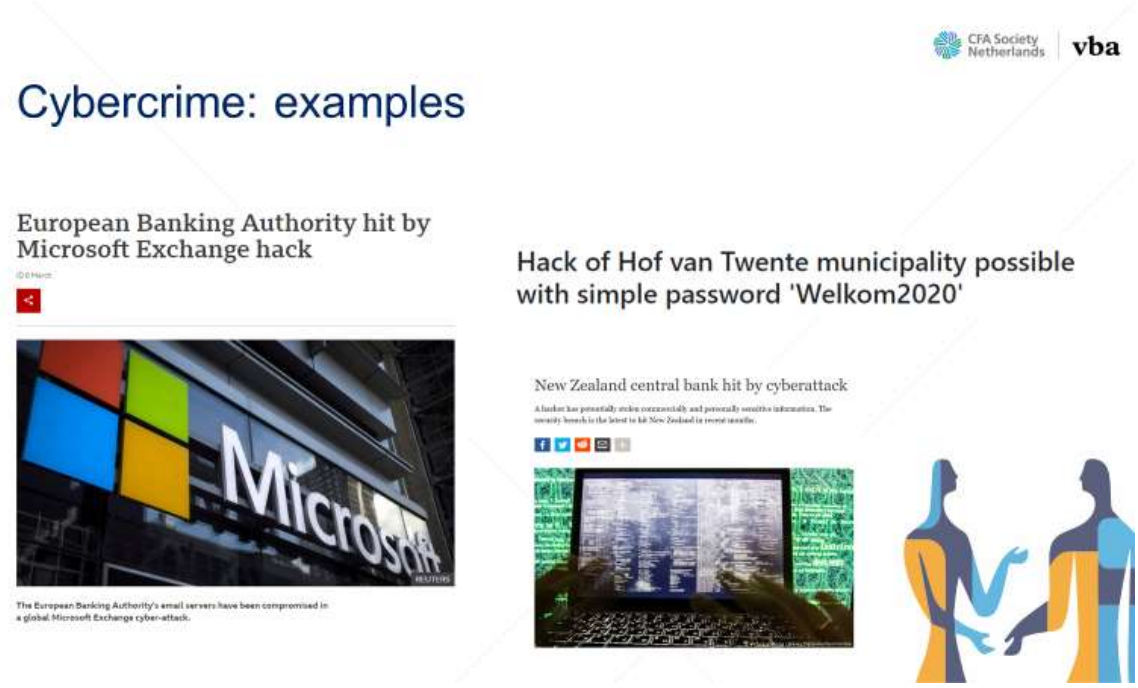
Some of the most common causes of cybercrime are: weak and stolen credentials (passwords), malware, phishing and insider threats. We'll show some examples.

Cybercrime: examples

Based on their research, PWC concluded in 2019 that asset managers are insufficiently aware of cybersecurity related risks. An example what could happen because of this is when information on the website of asset manager Nobel, now Oyens & Van Eeghen, was leaked, exposing personal client information to the outside world, where it could be used for criminal activities. This happened to The Reserve Bank of New Zealand, where a malicious breach of one of their data systems led to sensitive information being accessed illegally. Data leaks as such could potentially also damage the trust relationship with the client.

More recently, the European Banking Federation became the subject of a cyber-attack against Microsoft Exchange servers, forcing the organization to take their email systems offline.

Cybercrime could also take place on a smaller scale, while the effects could still be disastrous. In 2020, hackers were able to enter the computer systems of the Hof van Twente municipality through an easy-to-guess password: Welkom2020 and no two-step verification. The municipality's own system administrator created the password. The cyberattack severely limited the services of the municipality because data was destroyed and taken hostage.



We know that the costs of cybercrime are significant and risks for the financial sector are increasing. So what should asset management firms and other entities that have access to significant funds or client data do?

- First of all: The people using digital tools and client data should be educated on cybercrime and digital security as this is where hackers usually find their entry point.
- Then: Under MIFID II, companies need to ensure they have appropriate and proportionate systems, resources, and procedures in place, and must establish internal control mechanisms, effective procedures for risk assessment, and effective control and safeguard arrangements for information processing systems. This is an essential first line of defence. Regulators expect these to be in place and continually updated.
- Furthermore, MIFID II stresses the importance of having proper third party risk management: financial institutions should take reasonable steps to avoid additional operational risk coming from third parties, for example when a third party system is used for storing and maintaining sensitive information like personal client data. The New Zealand cyber-attack that we spoke about earlier is an example of this type of risk.
- Finally, companies also need to institute an action plan in the form of clear, thought-through policies and procedures to respond to cyber-penetrations when they occur. This should become part of a firm's general crisis management plan.

9. Consequences of violations

We have seen how different types of integrity risks could have major impact on a financial institution.

Violations of duties by financial institutions could have serious consequences, depending on how severe the breach or offence is. A distinction can be made between (a) consequences for the persons involved and (b) consequences for the firm itself.

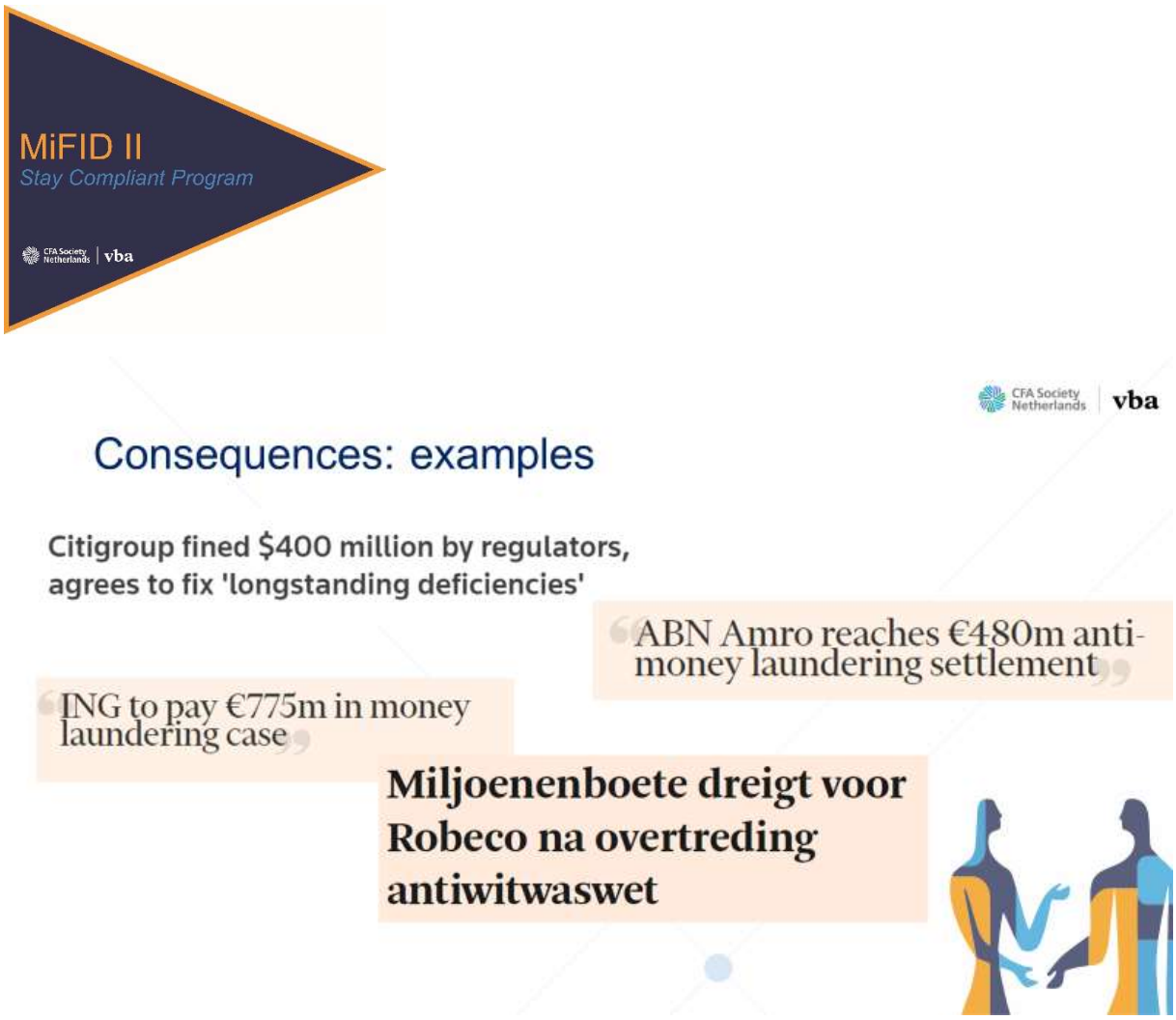
A firm can impose disciplinary sanctions against its employees, including remuneration related sanctions and if the breach or offence is serious enough it could lead to a termination of employment or even imprisonment. Depending on the nature of the breach or offence supervisors can determine that the person(s) involved are no longer trustworthy and therefore not suitable for the function they fulfil. If trustworthiness is one of the requirements to fulfil a certain position, this would mean that the person involved will no longer qualify for that respective function and should step down.

Both persons involved and the firm itself can be exposed to (financial) penalties, both from an administrative and criminal perspective. As we saw in the ABN AMRO case, also former employees can be subject to investigation.

For the firm such penalties could be connected to the firm's revenues, meaning that we are talking about serious numbers.

Consequences of violations: examples

The EUR 775 million penalty ING received in 2018 and the EUR 480 million penalty for ABN AMRO in money laundering cases are well-known examples of big penalties for financial institutions. The largest fine a financial institution received in recent years was the verdict of EUR 4.5 billion fine and damages in 2019 for Citigroup in France for not maintaining sufficient internal controls over its technology.



In other cases, supervising authorities could also threaten to impose a fine, which happened to asset manager Robeco recently. After being in breach of anti-money laundering and sanction regulation, Dutch supervisor AFM has threatened the asset manager with a EUR 1.8 million fine, unless they implement structural changes in their operational processes before the end of 2021. This relates to processes such as a proper customer due diligence and complete client records.

One final example of an imposed penalty applies to Citigroup, who received a USD 400 million penalty in 2020 for having structural insufficient internal controls and risk management. The decision for this penalty came 2 months after Citi transferred USD 900 million to one of their clients' creditors, an amount 100 times larger than it should have been, due to an administration error. A large part of this erroneous transaction has still not been transferred back to Citigroup. This incident has led to the CEO to resign earlier than planned.

When institutions fail to fulfil their duties as described in these examples, this brings a high risk of reputational damage and the same applies to the financial sector.

What should financial institutions do?

Governance

In servicing institutional investors, it is undoubtedly clear to be mindful of integrity risks and to act accordingly. The real life examples described earlier show how impactful violations of duties in this area can be.

Proper governance is one of the pillars used in safeguarding integrity in the financial sector. During the beginning of this century a lack of proper governance allowed financial institutions to take irresponsible risks leading to the Great Recession of 2008. Institutionalization of proper governance is achieved through a network of regulations that MiFID is part of. MiFID sets clear rules on governance to ensure that regulated investment firms operate with a high level of integrity, competence and soundness. It also links governance with other ethical and integrity related matters such as complaints handling, remuneration and conflicts of interest. Finally, MiFID stresses that organisations have sufficient procedures and controls in place for outsourced activities.

CFA Society Netherlands | vba

Governance means oversight and checks and balances and forms the heart of a firm's compliance organization. Everyone within a firm or working together with and on behalf of a firm should be subject to some form of oversight. To achieve transparency, investment firms should always provide sufficient information to their stakeholders; this enables accountability. Policies on procedures should be in place too.

Under MiFID II the senior management of a firm is responsible and accountable for the implementation, oversight, assessment and improvement of an effective governance system. Governance structures may vary, based on the size of the firm and the activities performed. It is important to recognize that there is no "one size fits all" approach. Governance is a dynamic aspect of a firm's organization and should therefore be subject to periodical review and adjustment.

This slide describes the governance related requirements for financial organisations when setting up their operational processes. I will not go through all points in detail, but what it is important that you know what firms must adhere to.

CFA Society Netherlands | vba

Compliance function

Firms should establish, implement and maintain a compliance structure that contains adequate policies and procedures designed to detect any risk of failure by the firm to comply with its obligations under the MiFID II and other applicable laws and regulations, as well as the associated risks. Firms should put in place adequate measures and procedures to minimize such risk. This requirement is intended to be proportionate, meaning that for different firms different levels of compliance can apply. Investment firms are required to consider the nature, scale and complexity of the business of the firm, and the nature and range of its investment services and activities.

Each firm should have a permanent and effective compliance function which operates independently, and which:

- monitors the adequacy and effectiveness of its measures, policies and procedures;
- advises the relevant persons responsible for carrying out investment services and activities to comply with the firm's obligations under the applicable laws and regulations;
- provides a report to the management board, on at least an annual basis (although it is advisable to do this more frequently, on the implementation and effectiveness of the overall control environment for investment services and activities, on the risks that have been identified, and on the complaints-handling reporting as well as remedies undertaken or to be undertaken;
- monitors the operations of the complaints-handling process and consider complaints as a source of relevant information.

Next to having a proper organisational governance and a compliance function, there are multiple other matters to pay attention to in preventing integrity risks.

A MiFID obligation that remains underexposed is the requirement to maintain a whistleblowing policy and to ensure that everyone within a firm is familiar with the policy and its existence. Whistleblowing remains something too often considered to be not done. Whistleblowing is one of the most effective manners to discover potential integrity risks within a firm. The policy should allow and enable employees to report anonymously on potential compliance breaches within the firm, also involving senior management members or compliance and risk officers.

Also, you should be aware of individual and group decision-making biases. One should realise a new normal may emerge that includes overriding existing controls, treating red flags as false alarms or accepting deviances and near misses. People may make investment decisions with overconfidence, meaning a false sense of their skills, talents or self-belief, leading to for example investments with too much risk. Another common bias when making investment decisions is to "throw good money after bad", also known as the sunk cost fallacy. This bias describes the behaviour of continuing with an activity, like investing in a certain product, simply because you have already put in resources.

CFA Society Netherlands | vba

Group decision-making biases may occur, e.g. the tendency to avoid critical evaluation of ideas the group favours. This is also referred to as group think. Group think can be avoided by having sufficient diverse management bodies in terms of age, gender, origin, education and profession.

Another example may concern an overconfident manager who wants to minimize conflict, delay, and challenges to his or her authority and the group accepting this behaviour.

Product suitability

The assessment of suitability is one of the key requirements for investor protection in the MiFID II framework. The importance of the suitability assessment for the protection of clients was already clear under MiFID I and has been confirmed under MiFID II.

ESMA has given three main guidelines for the implementation of suitability.

1. Information to clients about the purpose of the suitability assessment
2. Know your client and your product
3. Matching clients with suitable products and other requirements concerning qualification of staff and record-keeping.

Know your client and your product concerns

1. Arrangements necessary to understand the clients and to collect information from the clients
2. Updating client information
3. Client information for legal entities or groups
4. Arrangements necessary to understand investment products.

Matching clients with suitable products aims at

1. Arrangements necessary to ensure the suitability of an investment; and to take into account
2. Equivalent products (costs and complexity of equivalent products)
3. Costs and benefits of switching investments.

Relevant regulation

As mentioned earlier, it is crucial that you stay up to date on relevant national and international regulation.

The IORP II Directive is also included in Dutch pension fund regulation and compliance is secured by the supervisor. The directive aims to ensure a high level of protection for future pensioners (members and beneficiaries of pension funds) while guaranteeing efficient investment. Important elements in the directive include

1. Strict prudential rules
2. Investment rules adapted to the characteristics of IORPs and to the efficient management of savings
3. Rules permitting IORPs' cross-border activity, enabling the creation of pan-European pension funds.

The IORP II implementation in Dutch regulation also has clear requirements with regard to key functions. Key function holders must fulfil their role objectively, honestly and independently; and have access to relevant information.

The principle of the segregation of duties is also visible in the implementation of IORP II. Three main functions can be distinguished: the risk management function, the actuarial function and the internal audit function. In the Netherlands, the supervisor De Nederlandsche Bank sees to it that these functions are carried out independently. This has led to governance changes in the division of duties in Dutch pension fund boards and their executive offices.

IORP II helps pension fund boards to be On Task in line with good governance as we discussed earlier in this course.

The SIRA, the Systematic Integrity Risk Analysis, is aimed at strengthening the risk management capability of financial organisations. It is a legal obligation for e.g. pension funds, insurance companies, bank, trust offices and accountants. The SIRA is a joint effort of management, compliance and risk management. In 2020, the Autoriteit Financiële Markten (AFM) has investigated the quality of risk management at 15 investment firms. At 14 out of these 15 organisations, SIRA was not completely set up. After discussions with the board and compliance staff, these financial companies have put this in order.

Do's and don'ts

Now that we have discussed the impact of integrity risks and relevant areas to pay attention to, we will end this course by describing some practical do's and don'ts.

The most important thing to do is to be critical when dealing with clients when it comes to AML related tasks, but also if it involves compliance related matters in general. Ask clients questions (e.g. what would you like to achieve, did you consider other manners to achieve …, are these services for you or is it envisaged them to be beneficial to a wider group, is there a specific time element that we should take into account, is there a relationship with ...). But also ask questions to colleagues, managers, risk officers and compliance officers in the event that you are in doubt whether or not transactions or certain behaviour could have an impact on integrity. Transactions and behaviour may be justified, but it is always better to know for sure.

Never hesitate to bring concerns to the attention of the compliance or risk officer. In case you find it difficult to openly report to the compliance and risk officer, make use of the firm's whistleblowing policy. In the unlikely event that there is no whistleblowing policy in place try to escalate it to the senior management or other designated officers within a firm. Ensure proper recording and record keeping.

Celebrate working in a diverse group of people and last but not least: walk the talk.

Although it often feels good to just ignore signals, this would be the wrong thing to do. Integrity issues may not only have an impact on your organization, it will most likely have an impact on yourself as well. Ignoring signals may even have consequences for your own position, depending on your role and duties. Therefore in case of any doubt or concern: never ignore and take proper actions.

Continuing to facilitate trades, investments, transactions, etc. whilst it is obviously that by doing so the firm (and you) breaches applicable laws and regulations, even under the argument that you want to serve your clients interest, is an absolute no go, but in practise a mistake that is often made.

In case of AML: never inform the client about your doubts or notifications and reporting. This is not allowed under the applicable legislations and could lead to sanctions being imposed on the person(s) involved.

Given the crucial importance of IT: keep informed and make sure you do not postpone updates to protect your company for cybercrime.

**

Thank you for taking part in the module Integrity of Financial Markets of the 2021 MiFID II Stay Compliant Program of CFA Society VBA Netherlands. You can now take part in the multiple-choice assessment to test your knowledge and understanding. Good luck with the assessment!

CFA Society Netherlands | vba