Investigation Houston

Criminal investigation into ING Bank N.V.

Statement of Facts and Conclusions of the Netherlands Public Prosecution Service

OPENBAAR MINISTERIE

National Office for Serious Fraud, Environmental Crime and Asset Confiscation (Functioneel Parket) and National Office (Landelijk Parket)

Table of contents

Part I: Statement of facts

1. Introduction

1.1. Purpose and contents

This statement of facts describes how and why ING Bank N.V. became the subject of a criminal investigation by the Dutch Fiscal Information and Investigation Service (*Fiscale inlichtingen- en opsporingsdienst*, hereinafter referred to as FIOD) at the beginning of 2016, headed up by the Netherlands Public Prosecution Service (hereinafter referred to as the NPPS), under the name 'Houston'. The facts and circumstances that emerged from this investigation are set out in detail below.

1.2. Short description of ING

ING Bank N.V. is an internationally operating bank with a Dutch banking licence, which is part of the ING Groep N.V. (hereinafter referred to as ING Group). ING Group is listed on the AEX and NYSE stock exchanges. ING Bank N.V. provides financial services such as banking and investments. The bank's clients are private individuals, small and large companies, institutions, and government entities. ING Bank N.V. has offices in 40 countries and is headquartered in Amsterdam.

Banking services in the Netherlands are provided by and under the responsibility of the business unit ING Bank Nederland (hereinafter referred to as ING NL). ING NL, market leader in some areas in the Netherlands, has almost 9 million account holders in the Netherlands and processes approximately 340 million payment transactions per month (2017).

In addition, the Dutch Central Bank (*De Nederlandsche Bank N.V.*, hereinafter referred to as DNB) considers ING Bank N.V. to be one of the systemic banks in the Netherlands. The Financial Stability Board publishes an annual list of all the global systemic banks. ING Bank N.V. is the only Dutch bank on this list. Systemic banks are essential to the financial system and hence to the functioning of the economy and society.

1.3. Grounds for and course of criminal investigations

Several criminal investigations by the police and the FIOD into corruption and money laundering revealed that suspect persons and legal entities held one or more bank accounts with ING NL. Based on these findings, it was reasonably suspected that ING NL had violated several articles of the Anti-Money Laundering and Counter Terrorism Financing Act (*Wet ter voorkoming van witwassen en financieren van terrorisme*, hereinafter referred to as AML/CTF Act) and was guilty of money laundering and/or culpable money laundering. This behaviour gave rise to the suspicion that ING NL may have made money laundering by its clients (partly) possible. In the so-called tripartite consultation, a regular consultation that is held between, among others, the NPPS and DNB, it was decided to conduct a criminal investigation into these facts.

On 18 February 2016, the FIOD, led by the National Office for Serious Fraud, Environmental Crime and Asset Confiscation *(Functioneel Parket)* and the National Office *(Landelijk Parket)*, started a criminal investigation into ING NL under the name 'Houston'. As part of this investigation, an initial search of ING Bank N.V. was carried out on 1 March 2016. In the period that followed, various other seizures were made at ING Bank N.V. In addition, various data provision requests were issued to third parties for the purpose of obtaining data.

Shortly after 1 March 2016, ING Bank N.V. indicated to the NPPS that they were willing to cooperate with the investigation, and the NPPS concludes that ING Bank N.V. has indeed been cooperative. ING Bank N.V. also conducted its own internal investigations during the criminal investigation. ING's cooperation included the provision of relevant documents and information, which were involved in the assessment of the case by the NPPS.

2. Legal framework of the Anti-Money Laundering and Counter Terrorism Financing Act

2.1. Anti-Money Laundering and Counter Terrorism Financing Act (AML/CTF Act)

In order to have a clear understanding of the criminal behaviour that ING NL is accused of, this chapter explains the background and objective as well as the obligations under the AML/CTF Act[1] that are relevant for the criminal investigation.

2.2. Objective of the AML/CTF Act: to protect the integrity of the financial system

The AML/CTF Act was introduced in August 2008, in part as a result of the international fight against money laundering. The AML/CTF Act has its origins in the recommendations to combat money laundering that were made by the Financial Action Task Force on money laundering ('FATF'), an international partnership established by the G7 in 1989. It was considered crucial to protect channels through which the money laundering process can take place from being abused for criminal purposes. The disguising of the criminal origin of the proceeds of crime enables offenders to benefit from these assets undisturbed, and this undermines society.[2]

The starting point of the AML/CTF Act is described in Article 2a:
'In order to prevent money laundering and terrorist financing, an institution will conduct client due diligence and report unusual transactions that have taken place or are intended. (...) *In doing so, an institution shall pay particular attention to unusual patterns of transactions and to transactions which, by their nature, present a higher risk of money laundering or terrorist financing.'*

The purpose of the AML/CTF Act is to combat money laundering and the financing of terrorism and has four core obligations for the institutions that fall within the scope of this Act:

1. Carrying out a thorough client due diligence that is based on a risk assessment;
2. Reporting unusual transactions to the Financial Intelligence Unit of the Netherlands (FIU);[3]
3. Providing periodic training to employees so that they can identify unusual transactions and conduct client due diligence properly and completely;
4. Adequately recording the results of the risk assessment to be made available to regulators upon request.

Service providers therefore have a role to play in protecting the financial system against money laundering and terrorist financing, and thereby ensuring the integrity of the financial system. These institutions act as 'gatekeepers' protecting the integrity, stability, and reputation of the financial sector.

[1] This refers to the AML/CTF Act as applicable up to and including 24 July 2018.

[2] See Dutch Parliamentary Papers (*Kamerstukken*), Lower Chamber 2007-2008, 31 238, no. 3, pg. 1 and following.

[3] Organisationally, the FIU Netherlands is part of the national police force and is an independent body of the State of the Netherlands. Internationally, the FIU Netherlands is part of a global network of FIUs. The FIU analyses the unusual transactions that are reported and can make them available to various enforcement and investigation services as 'designated suspicious' (source: FIU.nl).

2.3. Applicable obligations from the AML/CTF Act

The criminal investigation focused mainly on the obligations under the AML/CTF Act to conduct (enhanced) client due diligence and to report unusual transactions to the FIU. These obligations are explained below.

2.3.1. Articles 3 and 8 AML/CTF Act: conducting (enhanced) client due diligence

The client due diligence to be conducted by institutions is also known as the Customer Due Diligence (CDD) screening. CDD also refers to the 'Know Your Customer (KYC)' principle. Article 3(1) AML/CTF Act obliges institutions to conduct client due diligence in order to prevent money laundering and the financing of terrorism. Article 3(2) AML/CTF Act describes the required results of this client due diligence. The legislator has opted for a principle-based approach; how the client due diligence should be carried out has not been outlined in detail, only what the result of the client due diligence should be. In a number of cases, the AML/CTF Act also prescribes enhanced client due diligence (Article 8 of the AML/CTF Act), for example in the case of a business relationship with politically exposed persons. Opening an account with a bank qualifies as a business relationship.

Client due diligence includes the following actions that banks are required to take during and after entering into a business relationship.[4]

- Identifying and verifying the client's identity;
- Identifying the client's ultimate beneficial owner (UBO) and taking risk-based, adequate measures to verify the identity;[5]
- Taking risk-based and adequate measures to understand the ownership and control structure of the client if it is a legal entity;
- Determining the purpose and intended nature of the business relationship;
- Performing ongoing monitoring of the business relationship and of the transactions carried out for the duration of that relationship in order to assess the institution's knowledge of the client and its risk profile, including, where appropriate, an examination of the source of the funds being used;[6]
- Determining whether the natural person representing the client is authorised to do so;
- Taking risk-based and adequate measures to verify whether the client is acting on its own behalf or on behalf of a third party;
- Determining whether the client is a politically exposed person (hereinafter referred to as a PEP) on the basis of risk-based procedures.[7]

Conducting client due diligence contributes to the recognition and management of risks associated with certain clients or certain types of service provision. Institutions should apply all client due diligence measures, but the intensity can be tailored to the risk posed by a particular type of client, relationship, product, or transaction. This is also referred to as the 'risk-based' approach; if the institution assesses the risks of money laundering or terrorist financing to be at a higher level, it must take additional measures.

---

[4] See also the '*DNB Leidraad Wwft en SW, Voorkoming misbruik financiële stelsel voor witwassen en financieren van terrorisme en beheersing van integriteitsrisico's*'.

[5] Until 1 January 2013, the obligation to identify the beneficial owner 'if applicable' applied; this phrase has been removed with effect from 1 January 2013 in order to clarify that an institution must always identify the beneficial owner or establish that the beneficial owner does not exist.

[6] Until 1 January 2013, the due diligence could include an examination of the client's assets rather than its source of funds.

[7] What is to be understood by a politically exposed person is described in Article 1(1)(e) of the AML/CTF Act.

Article 3(5) AML/CTF Act describes the cases, in addition to the point at which the relationship is entered into, where client due diligence must be carried out. This would be the case if, for example, there are indications of involvement in money laundering or the financing of terrorism and if the institution has doubts about the reliability of data previously obtained. The obligation to perform 'ongoing monitoring' as described in Article 3(2) AML/CTF Act also implies a (periodic) assessment date and keeping the information available about the client up to date. In other words: the client due diligence does not end after the client has been accepted by the bank.

It is necessary to determine whether a client is a PEP in connection with the obligation under Article 8 AML/CTF Act; an enhanced client due diligence must then be carried out. Relationships with PEPs require additional measures to address increased risks, as well as in the context of international anti-corruption policies.

An important measure that institutions should take to combat money laundering or terrorist financing by clients is the monitoring of client transactions in order to identify unusual transactions that, by their nature, present a higher risk of money laundering or terrorist financing. This is also known as post-event transaction monitoring, i.e. checking transactions that have already taken place. This is part of the obligation to conduct 'ongoing monitoring' of the client relationship and client transactions. Institutions can also structure this transaction monitoring process based on risk. This means that more attention is paid to transactions which, by their nature, represent a higher risk of money laundering or terrorist financing. The legislator leaves it up to the institutions to also shape this process themselves.

2.3.2. Article 5 AML/CTF Act: ban on entering into a relationship without client due diligence

Pursuant to Article 5 AML/CTF Act, an institution is prohibited from entering into a business relationship or executing a transaction on behalf of a client unless client due diligence as referred to in Article 3 AML/CTF Act has been carried out and the desired outcome has been achieved. Where an institution cannot meet the requirement of client due diligence in respect of an existing business relationship, it should terminate that relationship.[8] This is the case, for example, when the identity of the client is unknown. Institutions may not (or may no longer) provide services to that client.[9] In situations where there are considerable risks, no business relationship may be entered into, the transaction may not be executed, or the existing relationship must be terminated (at the next reasonable opportunity). Significant risks exist where it is impossible for an institution to identify the client or the beneficial owner or where the client is a legal entity that is part of a structure of international companies that is difficult to understand. Failure of the client due diligence can occur both during the client acceptance phase and during the business relationship.

[8] Until 1 January 2013, the obligation to terminate the business relationship was included in Article 5(1) AML/CTF Act. The obligation has been included in (2) as of that date.

[9] See the explanatory memorandum (*memorie van toelichting)* to the merger of the Dutch Identification in Services Act (*Wet identificatie bij dienstverlening)* and the Dutch Disclosure of Unusual Transactions Act (*Wet melding ongebruikelijke transacties*) (Wwft) , Parliamentary Papers (*Kamerstukken*), 31 238, no. 3, 16 October 2007, p. 20.

2.3.3. Article 16 AML/CTF Act: reporting of unusual transactions

Article 16 AML/CTF Act stipulates that institutions must immediately report any unusual transactions that are carried out or are proposed to the FIU after the institution has become aware of the unusual nature of the transaction.[10] This means that if there is reason to assume that a (proposed) transaction is related to money laundering or terrorist financing, an institution must report this to the FIU.

This obligation should be seen in conjunction with the obligation to conduct client due diligence. The various components of the CDD screening as set out above should, in combination but also separately, lead to unusual transactions being detected by institutions and then reported to the FIU in a timely manner. The monitoring of client transactions is an important means of identifying unusual transactions.

A transaction reported as unusual will then be further investigated by the FIU. This investigation may lead to the transaction being declared suspicious and to the investigating authorities being informed. In this way, reports of unusual transactions can lead to a criminal investigation into money laundering or the financing of terrorism.

[10] Before 1 January 2013, there was an obligation to report an unusual transaction that had been carried out or was proposed within fourteen days of the transaction's unusual nature becoming known.

3. Investigative findings

3.1. AML/CTF Act/FEC CDD policy at ING NL

As described above, the AML/CTF Act gives institutions the freedom in certain areas to implement the obligations in their organisation in a risk-based manner. The interpretation that ING Bank N.V. has given to the fulfilment/execution of its obligations under the AML/CTF Act is outlined in the so-called 'FEC CDD' policy.[11] This policy is applied to ING BANK N.V. worldwide by the compliance department at the head office of ING BANK N.V. in Amsterdam. The FEC CDD policy describes how ING Bank N.V. intends to carry out the obligations of the AML/CTF Act in its organisation and the efforts that the organisation must make to prevent money laundering and terrorist financing. In addition to guidelines, ING Bank N.V. has the 'FEC Minimum Standards', which apply worldwide to all ING Bank N.V. entities, and also operates local policies for each country that might be stricter in some respects. The FEC CDD policy at ING NL was subsequently fleshed out and elaborated on for so-called client segments. ING NL classifies clients into groups, the so-called client segments, on the basis of commercial classification criteria. For example, ING NL has a segment for private individuals, for high net-worth individuals, for small and medium-sized enterprises and for larger (listed) companies and multinationals. These client segments each have their own procedures and work processes, tailored to the risk of money laundering and terrorist financing that clients and products in that segment may entail.

ING NL uses the 'three lines of defence' model when drawing up and carrying out their FEC CDD policy. The ‘first line’ consists of the departments within the organisation that are responsible for the implementation of primary processes, the ‘second line’ is the compliance department, and the ‘third line’ is the internal audit service (CAS). The first line is responsible for carrying out the CDD process, with audits carried out by both the second and third lines.

ING NL's policy requires that, in addition to the CDD screening, clients be subjected to a risk assessment when entering into a relationship. Clients are assigned a risk classification: 'low', 'normal', 'increased', or 'unacceptable' risk. The assigned risk classification is important for, among other things, the periodic CDD investigations of the respective client (a so-called 'periodic CDD review'). In this case, the higher the risk, the more often a CDD review must take place. ING NL has also described certain ‘events’ in the policy. If these events occur, a CDD review must also be conducted. The risk classification that was previously assigned must then be re-evaluated. ING NL's policy is also that client data that is collected as part of a CDD screening must be kept for at least five years after the end of the relationship.

ING NL uses an automated system called Financial Crime & Risk Management (hereinafter: FCRM) for monitoring client transactions. In this system, defined criteria, called 'risk views' and 'alert definitions', determine whether transactions are selected for further investigation, after which the system creates a so-called 'alert', a sign that indicates a potentially unusual transaction (for example, a sign of money laundering). These alerts are then further investigated by handlers who manually check whether the transaction should actually be considered unusual. This investigation may ultimately lead to the FIU being notified of an unusual transaction and possibly other measures to be taken by the bank, such as assigning an increased risk classification or a decision to exit the client.

[11] FEC stands for Financial Economic Crime, CDD stands for Customer Due Diligence, as mentioned above.

3.2. Compliance with AML/CTF Act/implementation of FEC CDD policy at ING NL

The Houston investigation further investigated ING NL's actions in a number of cases in which ING NL's clients were suspected of committing criminal offenses. During this investigation, it was suspected that ING NL's actions with respect to these specific clients were not isolated incidents, but the result of structural shortcomings at ING NL in implementing the FEC-CDD Policy. In light of this, the investigation was expanded. This further investigation, based in part on documents requested from DNB, did indeed reveal shortcomings in the period from 2010 to 2016.

The following shortcomings were discovered:

1) the absence or incompleteness of CDD files;
2) the assignment of incorrect risk classifications;
3) not having the (periodic) CDD review process in order;
4) not terminating business relationships on a timely basis;
5) the insufficient functioning of the post-transaction monitoring system;
6) classifying clients into the wrong segments;
7) insufficient availability of qualitative and quantitative personnel capacity.

3.3. Missing or incomplete CDD files

The criminal investigation revealed that the client due diligence that ING NL is required to conduct when accepting clients was not done, or was done insufficiently, on a structural basis. For some clients, this was reflected in incomplete or missing CDD files. Shortcomings in the area of CDD files have been identified for the period from 2010 to 2016. For example, client identification and verification data and their UBOs were missing, possibly including PEPs, and ING NL was not, or not sufficiently, aware of its clients' activities. In order to comply with the legal identification requirement, ING NL had to carry out several remediation projects because the legally required information was not present in the CDD files. One of these remediation projects started in 2011 and concerned more than one million clients who had become clients prior to 2007. This project was largely completed in 2014.

This is also illustrated by the fact that, at the end of 2016, the internal audit service, CAS, found that ING NL had accepted new clients, both private and small and medium-sized business clients, in October 2016 without a CDD screening. This was due to errors in the onboarding process. ING NL's control systems had not previously identified these errors. This means that ING NL accepted clients without sufficiently investigating the risks associated with these clients. As a consequence, ING NL should not have accepted these clients.

The shortcomings in the CDD files were not found to only occur within a specific client segment, but occurred in all segments at ING NL. These segments also included high-risk clients, possibly including PEPs. In a number of cases, ING NL did not carry out an extensive CDD review until years after the client acceptance had taken place, after which it was decided to cut ties with a client who, for example, turned out to pose an unacceptable risk to ING NL. What played a role here was that ING NL wanted to offer its clients an attractive acceptance process that did not take sufficient account of the risks of doing business with undesirable clients. Not conducting client due diligence upon acceptance may result in undesired clients having been mistakenly accepted by ING NL and ING NL not having identified the risk of money laundering by clients upon acceptance. The AML/CTF Act therefore requires that clients may not be accepted if the client due diligence has not taken place or has not led to the required result (e.g. a complete client file).

3.4. Assigning incorrect risk classifications

The criminal investigation showed that ING NL regularly assigned incorrect or no risk ratings at all to some of its clients. No underlying documentation was requested or, where this did happen, no action or insufficient action was taken if clients did not provide the requested information.

This has to do, among other things, with to the fact that ING NL did not conduct any or conducted insufficient client due diligence at the time of entering into the business relationship, as described above. If the client is not subject to a client due diligence, a (correct) assignment of a risk classification cannot take place. After all, the risk of money laundering and terrorist financing can only be correctly assessed if the institution knows the client, the UBO, and the client's activities. The problem of assigning risk classifications also affected clients with a high risk of (involvement in) money laundering and corruption. PEPs are clients who are exposed to such high risks. A factor here is that if an institution has not identified its client or the beneficial owner, i.e. does not know its client, it cannot determine whether a business relationship is being entered into with a PEP and therefore whether enhanced client due diligence should take place.

Risk classifications have an impact on the measures ING NL takes to combat money laundering during the course of its business relationship. If no or incorrect risk classifications are assigned, a CDD review will, for example, not take place, or will be conducted too late. Another consequence is that monitoring of the client and transactions during the business relationship cannot be done properly, and the risk of signals of money laundering being missed is considerable.

3.5. Shortcomings in the CDD review process

ING NL's policy is that CDD reviews should take place after a certain period of time (depending on the risk classification) and if certain ‘events’ give cause to do so. These are the so-called periodic and event-driven CDD reviews. However, the FIOD's investigation revealed that neither form of review was conducted, or was conducted insufficiently. As a result, in many cases, ING NL did not check during the relationship whether the information known about the client was still correct or whether, for example, there was a change in ownership structure or in business activities. ING NL also often failed to take account of important signals which, according to their own policy, should have led to a CDD review. This concerned signals such as requests for information about clients coming from investigative authorities or signals coming from the company's own transaction monitoring system, FCRM. As a result, it was possible that ING NL could not identify signals of money laundering with regard to clients and therefore did not take sufficient measures.

3.6. Not terminating business relationships in a timely manner

The criminal investigation revealed that the ‘exit process’ for clients at ING NL was not in order. As a result it was possible that relationships with undesirable clients were not terminated in a timely manner. This was due to shortcomings in the processes and not complying with internal policy in the area of client exiting. Undesirable clients in this context include clients who are at risk of using ING NL to launder money. Because ING NL did not have the exit process in order, it was possible that, despite an insufficient and incomplete client due diligence (for example because information about the UBO was not disclosed), it did not sever ties with the client in a timely way.

3.7. Insufficient functioning of the transaction monitoring system

The criminal investigation revealed various shortcomings, including serious ones, in the transaction monitoring process at ING NL. This concerns shortcomings that relate both to the generation of alerts about client transactions by the transaction monitoring system, FCRM, and to the investigation and handling of these alerts by handlers. As a result, for many years, in the period from 2010 to 2016, ING NL did not take sufficient measures to identify unusual transactions and missed potential signals of money laundering.

In summary, this relates to the following shortcomings:

- The monitoring system settings, as a result of which many accounts were only monitored to a limited extent;
- The monitoring system settings which, for certain categories of money laundering signals, limited the system to a predetermined (in some cases very limited) daily number of alerts;
- The fact that, under the aforementioned settings, only percentage deviations in respect of the account history were taken into account in the selection and sorting of accounts for further investigation and not the absolute size of the transactions;
- Monitoring took place at account level and not at client level;
- Incomplete input of relevant data into the monitoring system for proper (and risk-based) monitoring;
- Insufficient (qualitative and quantitative) personnel capacity for handling alerts.

The settings were calibrated in such a way that many accounts were only monitored to a limited extent. When monitoring transactions, ING NL's method of limiting alerts was called 'capping' or 'topping'. The system was set up in such a way that each day, for certain categories of money laundering signals, after a predetermined maximum number of alerts (potential money laundering signals), the system stopped monitoring these categories of money laundering signals. The maximum number of alerts was limited to only three per day for several relevant categories of money laundering signals.

It has emerged that the maximum number of alerts produced by the system was to a large extent determined on the basis of the personnel capacity available at ING NL to investigate these signals in more detail. An internal ING NL recommendation on alert assessment, for example, states: *'Set* (...) *parameters to top off the (over)abundance of alerts and thus reduce the workload'.* In this context, the comment was made: *'is being done already*'.

In the 'topping' process, the selection and sorting of accounts for further investigation took into account percentage deviations from the account history and not the absolute size of the transactions.[12] By not checking this randomly and then adjusting the settings accordingly, ING NL's monitoring of its clients' transactions was insufficiently risk-based. As a result, there was a risk that appropriate, material transactions would not be selected for further analysis.

Furthermore, monitoring took place at account level and not at client level. In the case of a client with several bank accounts, monitoring was only carried out at the account level and not at the client level. The risk here is that so-called "smurfing" behaviour (where a large number of small(er)

[12] An example:

Transaction 1: if transactions for EUR 100 normally take place in an account and there is subsequently a transaction for EUR 10,000, the relative deviation is 100x;

Transaction 2: if the normal transaction behaviour of the account is EUR 1,000,000 and there is subsequently a transaction for EUR 99,000,000, there is a relative deviation is 99x.

This system ranks Transaction 1 higher on the list of unusual transactions.

transactions are deliberately spread across several ING NL bank accounts held by the same client) is not noticed/recognised.

Finally, the last factor in this respect is that ING NL did not investigate the effectiveness of its transaction monitoring system and did not keep it up to date for the period from 2010 to 2016, and that ING NL barely adjusted its criteria to take developments in the area of money laundering and increasingly strict legislation and regulations into account.

3.8. Incorrect client segmentation

Within ING NL, clients are classified into so-called 'client segments' on the basis of commercial classification criteria. Each client segment within ING NL then has its own measures to combat money laundering and terrorist financing, adapted to the type of client and products offered in that client segment. That is why it is important to classify a client in a certain client segment using the proper grounds.

The investigation showed that ING NL did not have sufficient control over the correct 'segmentation' of its clients. This was due to the fact that ING NL based the segmentation process on the client's information, and that during the business relationship, ING NL did not monitor whether clients had been assigned to the right client segment, for example by checking during the relationship whether the turnover was still appropriate for the client segment in question.

This resulted in a high risk of involvement in money laundering, because high-risk clients could end up in client segments where measures to combat money laundering (such as the extent of the client due diligence and the transaction monitoring method) were less stringent because the risks in that client segment were estimated by ING NL to be lower. An example of a high-risk client is a so-called trust client, i.e. a Dutch company owned generally by a foreign client and managed by a Dutch trust office. These types of companies are also referred to as 'special purpose vehicles'. Special purpose vehicles are often part of complex ownership structures and are often used in structures involving international financial flows and for these reasons carry a higher risk of money laundering. It was shown that such clients could be misclassified into the wrong client segment.

Another consequence of an incorrect segmentation is that ING NL's transaction monitoring system is not 'triggered' by unusual transactions made by the client in question. This is because the transaction monitoring system uses different criteria for each client segment to identify a transaction as unusual.

3.9. Lack of qualitative and quantitative personnel capacity

The criminal investigation revealed that ING NL had struggled with personnel capacity problems for many years in the departments relevant to compliance with the AML/CTF Act, such as the departments that conducted CDD reviews and departments where employees worked on investigating signals of money laundering from the transaction monitoring system. Not enough staff capacity was made available to carry out the work and also to solve the problems that had become known within the organisation in an expedient and structural way. Also, the available staff did not always have the necessary knowledge and experience to do the work. The investigation showed that ING NL did not invest enough in personnel capacity and quality in the period from 2010 to 2016.

3.10. Causes of the shortcomings

The criminal investigation revealed several underlying organisational causes that led to the serious and repeated shortcomings in ING NL's compliance with the AML/CTF Act.

- Insufficient attention & priority

For many years, insufficient attention was paid within ING NL to the correct carrying out of the FEC CDD policy. There was a lack of awareness, also among the senior management involved, of the importance of soundly carrying out of this policy. There was also a lack of awareness about the extent to which ING NL continued to underperform in terms of meeting its legal obligations for many years; the 'tone at the top' did not sufficiently buy into the importance of the proper carrying out of AML/CTF Act obligations. For many years, insufficient investments were made in operating the transaction monitoring system and in the capacity of the personnel involved in handling signals of money laundering generated by this system, both in respect of numbers and level of education.

- 'Business over compliance'

The Houston investigation showed that in certain (investment) decisions, commercial objectives prevailed over compliance with the AML/CTF Act. This had an effect on the work processes within ING NL, for example when accepting clients. The awareness that compliance is important and thinking in terms of compliance was not sufficiently embedded in the ING NL organisation.

- No sustainable solutions

Within ING NL, several improvement programmes aimed at FEC CDD, and compliance in a broader sense, were implemented. However, insufficient will and drive were shown within the organisation to solve the problems in a sustainable manner. This led to problems being solved in the short term, but not to good solutions being worked on for the future, meaning that culpable shortcomings persisted.

- Dysfunctioning of internal controls and fragmentation

A major cause of the occurrence and persistence of the shortcomings was the dysfunctioning of internal controls within ING NL in respect of compliance risk management. ING NL used the 'three lines of defence' model as described above. All these 'lines of defence' had their own role to play in preventing non-compliance with laws and regulations. The criminal investigation revealed that these 'lines of defence' felt limited responsibility for the whole and that this was a case of fragmentation in which everyone focused only on their own specific role and therefore lacked ownership of the entire process.

- Absence of an escalation culture

During the investigation it became clear that the way in which ING NL's FEC CDD policy was carried out lacked a culture in which problems were escalated upwards in the organisation. Significant shortcomings that were known to ground-level employees, for example, did not or barely penetrate through to the senior management. Signals that did reach the senior management (e.g. also signals from DNB), were subsequently assigned to the ground level without sufficient monitoring of remediation measures.

4. Consequences of serious shortcomings in implementing the FEC CDD policy

4.1. Scope of problems and consequences

As described above, the investigation revealed that ING NL demonstrated serious shortcomings in the implementation of its FEC CDD policy in the years 2010 - 2016.

It must be concluded that ING NL missed a significant number of money laundering and corruption signals over a number of years as a result of inadequately carrying out the FEC CDD policy. It is not known exactly how many signals were missed, and ING NL essentially no longer has the ability to determine these numbers.[13] However, based on the number of clients at ING NL and the number of transactions carried out, the number of infringements during the investigation period must have been very significant. Furthermore, it is not known how many clients who engaged in criminal activities ING NL would have been able to identify if it had correctly carried out its FEC CDD policy. As a result, it is not possible to determine how much money has actually been laundered over the years via ING NL's bank accounts. Nor is it possible to give any indication of the number of transactions that may have been related to other financial-economic crime that took place using ING NL's client accounts. The investigation justified the suspicion that there had been a large number of unusual transactions that ING NL had not identified. Reference is made to an ING NL internal memorandum:

> *'For years we have only monitored the tip of the iceberg without taking samples of the remaining alerts, which could have given us an idea of the quality and effectiveness of our monitoring programme and the risk views used in it, i.e. which could or should have led to adjustments to these risk views.'*

As a result, ING NL insufficiently fulfilled its gatekeeper role and insufficiently enabled investigative authorities to take action. Also, shortcomings in carrying out the FEC CDD policy led to a number of clients being able to use ING NL's accounts for years almost undisturbed for, among other things, money laundering.

During the investigation, FIOD received dozens of concrete signals and indications regarding ING NL clients indicating that ING NL may have been guilty of criminal offenses. A number of these signals, which were investigated extensively and in which criminal offenses were detected, are described in section 4.2.

4.2. Description of specific examples/cases

The criminal investigation has shown that the inadequate implementation of the FEC CCD policy actually led to misuse of ING NL's accounts by criminals. The cases described below, which serve as examples, show this.

- A company has been accused of laundering many millions of euros on Curacao for third parties. This money laundering scheme was run through a bank account held with ING NL. From May 2010 up to and including 2014, this bank account was funded with approximately €150 million in credit card transfers. The FIOD found that ING NL did not know the client sufficiently during the client relationship; the identity of the UBOs and the business activities appeared to be insufficiently clear from the CDD file at relevant moments (e.g. in the case of alert handling). Also noteworthy is the classification in the small and medium-sized businesses segment. ING NL did not notice the fact that the bank

[13] The monitoring system does not record any results. In order to make a re-examination, all the hundreds of millions of historic transactions from the period in question would have to be reloaded into the monitoring system.

account was subsequently funded with €150 million. ING NL's transaction monitoring system generated a total of 49 signals of money laundering (alerts) from 2010 to 2013, all of which, almost without further investigation, were dismissed by ING NL as 'not suspicious'. Even during that time, the actual business activities remained unclear and ING NL did little to verify vague and evasive responses by the client in this respect. Another bank and other service providers were already checking out this Curacao company. That other bank also asked ING NL questions in this respect. The first FIU report was not received from ING NL until 1 August 2013, more than 3 years after the first alert from July 2010. Eventually, ING NL started the exit process for this client in August 2014 and the relationship was actually terminated shortly after 1 January 2015.

- A one-man business is suspected of 'underground banking' and money laundering for third parties. This took place in the years 2013 up to and including 2015 via a bank account held with ING NL. On paper, the one-man business was a trader in building materials and only had an address in Suriname. In fact, however, it was a currency exchange office in Suriname. In order to launder their money, clients paid for a purchase from the one-man business via a PIN terminal in Suriname, but in reality they were paid an amount in cash. ING NL carried out practically no client due diligence at the time of acceptance, as a result of which 15 mobile ATMs (PIN terminals) were connected to the bank account of the one-man business for use in the Netherlands, even though on paper the client did not carry out any activities in the Netherlands. The total volume of transactions for this one-man business that took place in the bank account starting in 2013 amounts to more than €9 million. In April 2015, ING NL blocked the PIN terminals. On 15 September 2015, ING NL informed the client that no more transactions had taken place on the account since the end of April 2015, that the PIN terminals would no longer be activated, and asked whether the client wished to keep the account. The client then requested the termination of the account, which was then effectively terminated on 18 September 2015.

- Another client relationship concerned an authorised representative for the bank accounts of two companies (F and A). On paper, these companies were importers and traders of fruit and vegetables from South America. However, following a police investigation, however, this turned out to be a cover. During the investigation, the FIOD found that ING NL did not have a copy of the identification document of the owner of the companies available in the client's CDD file available. The authorised representative for the account turned out to be a bankrupt person known to ING NL. From the time the account was opened, numerous high-volume cash deposits were made into the bank account of F and A, including in €500 banknotes. Up to and including January 2015, a total of ninety cash deposits took place for a total amount of €343,035 into F's account. The transaction monitoring system did not raise a single money laundering alert at ING NL for client F. From September 2014 up to and including February 2015, a total of 41 (high-volume) cash deposits were made onto A's account for a total amount of €164,530. The majority (95%) of the deposits were made after the above-mentioned bankrupt person became an authorised representative on the bank account. On 12 November 2014, a request relating to A was sent to ING NL by the police. On 1 December 2014, the transaction monitoring system generated one alert for cash deposits into A's account. The relationship with company A was terminated at the end of May 2015. In June 2015, ING NL decided to terminate its relationship with company F, as well.

- Vimpelcom has entered into a settlement agreement with the NPPS in connection with the payment of bribes to Karimova, the daughter of the former President of Uzbekistan. These bribes were paid out from the bank account that Watertrail, a subsidiary of Vimpelcom, held with ING NL. Watertrail paid a total of $55 million in 2007 and 2011 to Takilant, a Karimova-affiliated company based in Gibraltar. Essential data on Watertrail's UBO was

missing. As early as 2012, after the transactions had taken place, ING NL received numerous signals from public sources that Takilant had been linked to Karimova's money laundering and corruption practices. ING NL's transaction monitoring system did not generate an alert for any of the transactions in 2007 and 2011. In April 2015, ING NL reported Watertrail's payments to Takilant as unusual transactions to the FIU. ING NL only did this after a journalist asked specific questions about the transactions.

FIOD has identified several other similar signals coming from criminal investigations or from the media. These signals have not been investigated in detail, but confirm the existing picture of ING NL falling short in carrying out the FEC CDD policy and the associated risks of money laundering by clients.

PART II: Conclusions of the NPPS

5. Serious nature of the facts

5.1. Introduction

Chapter 4 sets out the consequences of the serious shortcomings in the implementation of ING NL's FEC CDD policy. As a result, ING NL structurally breached the law and was guilty of a large number of criminal offenses. For several reasons, the NPPS is of the opinion that this can be qualified as very serious.

5.2. Systemic bank

ING Bank N.V. is a large internationally operating financial institution. Hundreds of millions of transactions are processed through its accounts every month.

As a systemic bank, ING Bank N.V. also bears a great responsibility, a responsibility that goes beyond clients or shareholders. It shares responsibility for the reliability of our financial system and can and should make an important contribution to the integrity of that system. ING NL can therefore also be expected to act in a socially responsible manner and to uphold integrity.

In addition, ING NL enjoys a good reputation. Once a payment is passed through an ING NL account, the payment can most likely be viewed as approved, and in national and international trade people generally rely on it.

5.3. Gatekeeper function

ING NL has an important gatekeeper function in the fight against all kinds of financial and economic crime. The legislator has also explicitly assigned this task to institutions such as ING NL. The explanatory memorandum (*memorie van toelichting*) to the AML/CTF Act is clear on this point and states that institutions must take reasonable measures, proportional to the nature and size of the institution, to determine and assess the risks of money laundering and the financing of terrorism. The gatekeeper function means that a bank should, where necessary, identify undesirable elements in our financial system, prevent them and counteract or report undesirable transactions. This is because banks are ideally placed to detect indications of money laundering, as they have an overview of clients' transactions. Compliance with the AML/CTF Act is intended to prevent the financial system from being misused, for example, for the purpose of laundering criminal money.

The bar is therefore high for an institution like ING NL in terms of what can and should be expected of it in this respect, and ING NL must take its legal obligations seriously. For years, however, ING NL has not complied with its obligations under the AML/CTF Act, or has complied with them in a completely insufficient manner.

5.4. Business over compliance

The investigation revealed that ING NL has structurally under-invested in meeting its legal obligations over a long period of time. One of the reasons for this was that when carrying out the FEC CDD policy, compliance was often considered to be less important than the business. ING NL's focus was mainly on the profitability of the organisation and reaching its commercial objectives. The lack of investment in the necessary capacity, both in personnel and in technical terms, has contributed to the emergence and continuation of serious shortcomings in implementing the FEC CDD policy. Internal signals from the ground level employees did not or did not sufficiently reach the senior management. The senior management lacked the right 'tone at the top' for FEC CDD: its importance was not sufficiently understood or communicated, as a result of which, for example, there was no real and consistent drive to sufficiently implement the FEC CDD policy.

5.5. Insufficient measures taken after internal and external warnings

Over the years, various external bodies, namely DNB and the European Central Bank (hereinafter the ECB), have drawn ING NL's attention to shortcomings and risks in the way it was carrying out its FEC CDD policy. Internally, too, it was noted on several occasions that the required FEC CDD policy had not been carried out at all adequately. However, all these signals did not lead to any substantial changes. Although some internal remediation projects were started and carried out by ING NL, they never led to a sufficient degree of compliance with AML/CTF Act obligations.

In the period from 2005-2016, DNB conducted a number of investigations at ING NL, including investigations into ING NL's prevention of involvement in money laundering and terrorist financing. DNB took formal measures against ING NL on a number of occasions during that period. In 2008, for example, the DNB imposed an instruction on ING, which aimed to *'satisfy the requirements that ensure the controlled and sound operation of the business*'. As a result, ING NL was aware of the need for extra attention to be able to carry out its FEC CDD policy properly. Following the instruction imposed by DNB, ING NL set up a broad compliance improvement programme, which included FEC CDD. In addition, in 2015, the DNB imposed the formal enforcement instrument by means of an order for incremental penalty payments on the private banking division of ING NL for non-compliance with the AML/CTF Act obligation to conduct sufficiently in-depth client due diligence. In 2016, the DNB also reported various shortcomings in the post-event transaction monitoring process to ING NL. Both before and after the instruction and the order for incremental penalty payments were imposed, on a number of occasions, DNB drew ING's attention to shortcomings in the implementation of the FEC CDD policy and the associated risks to ING NL with respect to complying with its AML/CTF Act obligations.

In addition to DNB, the ECB has also drawn ING Bank N.V.'s attention to risks in the compliance organisation and compliance function. The compliance function is charged with and responsible for monitoring the carrying out of the FEC CDD policy. For example, following an on-site investigation in 2015, the ECB reported various findings on the functioning of the general compliance function within ING Bank N.V., identified various risks, and made recommendations.

The problems that the criminal investigation has revealed in the area of compliance with AML/CTF Act regulations at ING NL are essentially the same as those that had been identified on a regular basis, both internally and externally, since 2008.

5.6. Conclusion

The objective of the AML/CTF Act is to combat money laundering and the financing of terrorism. Service providers are required to protect financial transactions against money laundering and terrorist financing, thereby ensuring their integrity. In doing so, these institutions act as gatekeepers protecting the integrity, stability, and reputation of the financial sector. This applies in particular to a systemic bank such as ING Bank N.V.

The investigation has revealed that, at ING NL, despite various warnings, there were and remained structural and serious shortcomings in the implementation of the FEC CDD policy. It must be concluded that, as a result, ING NL missed an expected large number of signals of money laundering during the period from 2010 to 2016. ING NL has failed in its gatekeeper function and, as a result, has not sufficiently enabled investigative authorities to take action in response to unusual and suspicious transactions.

The serious shortcomings in the implementation of the FEC CDD policy have meant that some clients who engaged in criminal activities were able to use bank accounts held with ING NL virtually undisturbed, for years. A number of examples of the ease with which this could take place have already been outlined in section 4.2 above. It is clear, however, that these examples are only

illustrative and that due to the way in which ING NL did (not) comply with the AML/CTF Act in the years 2010 to 2016, it missed signals of money laundering.

During the investigation, the FIOD received dozens of signals and indications regarding ING NL clients indicating that ING NL may have been guilty of criminal offenses. An internal investigation by ING NL also shows that ING NL did not comply with the AML/CTF Act and that there are indications of money laundering by its clients. Based on the number of clients that ING NL has and the number of transactions carried out by its clients, it is likely that the number of AML/CTF Act infringements and missed signals of money laundering during the investigation period must have been very significant. It is not known how many clients who engaged in criminal activities ING NL would have been able to identify if it had carried out its FEC CDD policy correctly. As a result, it is not possible to determine how much money has actually been laundered over the years via ING NL's bank accounts. Nor is it possible to give any indication of the number of transactions that may have been related to other financial and economic crimes.

6. Criminal allegations against ING

6.1. Criminal offenses

In view of ING NL's actions as described above, the NPPS is of the opinion that, in the period from 1 January 2010 up to and including 31 December 2016, ING NL was guilty of violating a number of provisions of the AML/CTF Act in the Netherlands, on multiple occasions, on a habitual basis.[14] ING NL was also guilty of culpable money laundering, which is made punishable by Article 420quater of the Dutch Criminal Code, on several occasions during this period.

6.2. AML/CTF Act

With regard to the AML/CTF Act, this concerns a violation and/or non-compliance with the following articles:

- Article 3 AML/CTF Act, which requires an institution to conduct client due diligence in order to prevent money laundering and the financing of terrorism;
- Article 5 AML/CTF Act, which prohibits an institution from entering into a business relationship or carrying out a transaction if it has not conducted any or has not conducted a satisfactory client due diligence. Article 5 AML/CTF Act also requires an institution to terminate a business relationship with a client if the institution is unable to comply with the provisions of Article 3(1) and (2), preamble and (a), (b) and (c);
- Article 8 AML/CTF Act, which requires an institution to conduct enhanced client due diligence in certain cases;
- Article 16 AML/CTF Act, which requires an institution to report unusual transactions to the FIU within two weeks/immediately after the unusual nature of the transaction has become apparent.

The NPPS is of the opinion that ING NL's violations of the abovementioned articles qualify as criminal offenses, pursuant to Article 2(1) of the Dutch Economic Offenses Act (*Wet op de economische delicten*). Furthermore, with reference to Article 6(1)(3) of the Dutch Economic Offenses Act, ING NL committed these offenses on a habitual basis.

6.3. Culpable money laundering

The obligations under the AML/CTF Act described in chapter 2 form a coherent set of measures aimed at preventing money laundering. The AML/CTF Act is crystal clear on this point; these measures are required of ING NL in order to combat money laundering through its bank accounts.

Over the years, from 2010 to 2016, ING NL has fallen short in taking these measures in such a way that, in the NPPS's opinion, ING NL has not done what can be expected of a financial institution to prevent money laundering by clients through its bank accounts. As described in detail in chapter 3 of this report, ING NL's (transaction monitoring) systems, processes, and resources were completely insufficient. In the eyes of the NPPS, ING NL knew that it was making insufficient efforts to meet its legal obligations to combat money laundering by its clients and nevertheless neglected to make further efforts.

ING NL should have reasonably suspected that some of the cash flows through its clients' bank accounts originated from some form of crime. As described in sections 4.1 and 4.2, ING NL received several signals about specific clients that should have resulted in a suspicion of money

[14] As of 1 January 2015, the Dutch Economic Offences Act (*Wet op de economische delicten*) criminalises habitually committing an economic offence that qualifies as a crime (*misdrijf*).

laundering. Examples include unusual transactions that do not fit in with the nature of the business, vague and unusual statements regarding the origin of funds, signals from public sources of money laundering relating to clients, requests for information from the police and the FIOD, alerts from the transaction monitoring system, high-volume cash deposits, queries from correspondent banks, and information from the FIU and Equens about its clients' involvement in money laundering. It is clear, however, that these examples, as already mentioned in chapter 5, are only illustrative. Due to the way in which ING NL did (not) comply with the AML/CTF Act in the years 2010 to 2016, it often missed signals of money laundering. The fact that ING NL was repeatedly unable to bring these signals together effectively and to act on them sufficiently can and must be attributed to ING NL. These circumstances have led to ING NL being accused by the NPPS of culpable money laundering.

6.4. Attribution of offenses to the legal entity/organisation

The criminal investigation revealed that responsibility for compliance with the AML/CTF Act lay with three different divisions of ING NL. These were the 'business', 'compliance', and internal audit, or 'CAS', departments. None of (the employees of) these units felt responsible for and oversaw the entire picture. Many were jointly responsible for part of the culpable behaviour. In particular, the lack of internal controls within ING NL on compliance risk management was a major cause of the criminal offenses. The NPPS qualifies the identified conduct as illegal acts carried out by a legal entity within the scope of its normal business operations.[15] When attributing the offenses committed, the organisation takes precedence over the individual.

The Dutch Supreme Court (*Hoge Raad*) sets a high bar for prosecuting individuals for directing offenses such as those identified at ING NL; not only must there be proof that these individuals knew of offences, but these persons must also have consciously contributed to the committing of criminal offenses by the organisation or consciously neglected to prevent them. The investigation showed that, in the period from 2010 to 2016, several individual current and former employees and managers at ING NL made mistakes. However, the NPPS is of the opinion that the investigation has not produced sufficient evidence to make criminal accusations against these individuals. The NPPS is therefore attributing the offenses to the organisation as a whole.

[15] Also known as criminal offenses attributable to legal entities ("*organisatiecriminaliteit*").

7. Decision to reach a settlement

7.1. Statement of reasons

Before the start of the hearing, the NPPS may set out one or more conditions which must be satisfied to avoid criminal prosecution for crimes (*misdrijf*) punishable by imprisonment of no more than six years and for minor offenses (*overtredingen*) (Article 74 of the Dutch Criminal Code). In other words, the settlement is an option provided for by law to settle criminal cases outside the courts.

In this case, given the size of the settlement amount, it is considered a high settlement. It is also a special settlement at a time when, among other things, the general functioning of the financial and economic sector is at stake. Such a settlement is subject to the "Designation Order for High Settlements and Special Settlements" (*Aanwijzing hoge transacties en bijzondere transacties*) (http://wetten.overheid.nl/BWBR0024648/2008-11-01).

The aforementioned designation order includes the basic principle: *"not to settle in such cases (but to submit them to the courts), unless there is a very good reason for doing so*". In the Houston criminal investigation there are good reasons for settling, namely:

- ING NL publicly acknowledges and regrets the mistakes made;
- ING NL cooperated in the criminal investigation and investigated the matter internally and the outcomes have been reported to the NPPS;
- ING NL will continue to actively allow the NPPS to investigate possible criminal offenses arising from shortcomings in the FEC CDD policy to which the settlement relates;
- ING NL, under the supervision of DNB, has developed and implemented a remediation plan. ING NL also provided the NPPS with insight into the progress of this remediation plan throughout the criminal investigation;
- As part of this settlement, ING NL is taking responsibility for criminal offenses committed over a period of several years.

For these reasons, the NPPS considers a settlement to be more effective than court proceedings.

Part of the settlement is the imposition of a € 675 million fine. ING NL has accepted this penalty. ING NL will also pay an amount of € 100 million for unlawfully obtained gains. This is explained in more detail in chapter 8.

7.2. Cooperation with the investigation

After becoming aware of the Houston investigation, ING NL cooperated with this investigation. For example, ING NL has actively cooperated in making documents relevant to the investigation available and has made efforts to make witnesses available for questioning at short notice.

7.3. Acknowledgement of mistakes

ING NL has publicly acknowledged the mistakes made in the past. The press release they issued on 4 September 2018 demonstrates that sufficiently, in the NPPS's opinion.

7.4. The remediation measures taken and the remediation plan under the supervision of DNB

ING NL developed a large-scale remediation plan during the criminal investigation and started implementing it. The aim of this long-term remediation programme is to tackle the identified

shortcomings in an expedient and sustainable manner and to remedy them permanently for the future. The development, carrying out, and progress of the aforementioned remediation plan will be put into place over several years and are being supervised and monitored by DNB. The NPPS considered this reason enough to agree to a settlement for the period from 1 January 2010 to the date the settlement agreement is signed.

8. Conclusion of the criminal investigation

8.1. Contents of the settlement agreement

The settlement agreement between the NPPS and ING Bank N.V. has been made public in its entirety.

8.2. Penalty and unlawfully obtained gains

ING NL will pay a total of € 775 million to the Dutch State as part of this settlement. This amount consists of a fine of € 675 million and the confiscation of unlawfully obtained gains amounting to € 100 million.

8.2.1 Fine

In determining the amount of the fine, the fact that only a significant fine does justice to the seriousness, extent, and duration of the offenses uncovered was taken into account. The amount of the fine also reflects the fact that it was not possible to determine how much money had actually been laundered through ING NL's bank accounts over the years, nor was it possible to give an indication of the number of transactions relating to other financial and economic crime that had been carried out via client's bank accounts. Consideration has also been given to the repeated warnings and signals issued both internally and by regulatory bodies. In determining the fine to be imposed by the NPPS, the financial capacity of the defendant, as intended by the legislator, was also taken into account:

> *"In addition to the seriousness of the offense and its benefit, a third factor plays an important role in determining the amount of the fine for an offense under criminal law: the offender's capacity to pay. Financial-economic crimes are often committed by companies that have sizable assets, relative to private persons. The capacity of legal entities is therefore important in determining whether a fine has a sufficiently deterrent effect.*[16]

A fine should therefore have a deterrent effect and have an impact on the legal entity. This means that a higher fine is appropriate in the event that a legal entity has a greater capacity to pay.

Taking all facts and circumstances into account, the NPPS considers a fine of € 675 million to be appropriate. In determining the amount of the fine, the NPPS took into account ING NL's recognition of the mistakes made, ING NL's cooperation with the investigation, and ING NL's remediation activities aimed at correctly carrying out the FEC CDD policy.

8.2.2 Unlawfully obtained gains

As part of the settlement, an amount of € 100 million for unlawfully obtained gains was confiscated. ING NL did not have sufficient personnel to comply with its AML/CTF Act obligations in the period from 2010 to 2016. The amount ING NL has unjustly saved as a result has been set at € 100 million.

[16] Explanatory memorandum (*memorie van toelichting*) to the introduction of the Act 'Expanding the possibilities of combating financial and economic crime' (*Wet 'verruiming mogelijkheden bestrijding financieel-economische criminaliteit'*); Parliamentary Papers (*Kamerstukken*), 2012-13, 33 685, no. 3, pg. 9-10.