# CENTRALE BANK VAN CURAÇAO EN SINT MAARTEN
# (Central Bank)

# Provisions and Guidelines

# for

# Safe and Sound Electronic Banking

---

*WILLEMSTAD, Updated version April 2011*

# Provisions and Guidelines for Safe and Sound Electronic Banking

# I. Introduction

In its continuous effort to promote and ensure safe and sound banking practices on the islands of Curaçao and Sint Maarten, the Centrale Bank van Curaçao en Sint Maarten ("the Bank") hereby issues the "**Provisions and Guidelines for Safe and Sound Electronic Banking"(hereafter "Provisions and Guidelines")**.

Ongoing innovations in information technology and competition among banking institutions, new market entrants, and mergers and acquisitions have contributed worldwide to a wider array of electronic banking ("hereinafter e-banking") products and services. The islands of Curaçao and Sint Maarten have also experienced this development amongst its credit institutions, and the acceptance of e-banking services has grown rapidly.

E-banking carries benefits as well as risks to credit institutions. Because the characteristics of e-banking increase and modify banking risks and thereby influence the overall risk profile of banking, the Bank finds it important that these risks be recognized, addressed, and managed by the relevant credit institutions in a prudent manner.

Worldwide fraud, identity theft, money laundering, and terrorist financing also frequently are incline to move to countries where credit institutions provide e-banking products and services and which have inadequate risk management regarding e-banking. Therefore, the Bank recommends that credit institutions adopt relevant policies and stronger risk management including internal control to prevent these kinds of immoral activities.

These Provisions and Guidelines provide credit institutions, which are subject to the Bank's supervision, with guidance on the general principles for risk management of e-banking[1] and outline suggestions for consumer security and education. The Provisions and Guidelines should help credit institutions to expand their risk oversight policies and processes to cover their e-banking activities.

The "Provisions and Guidelines" are particularly derived from the principles and recommendations for e-banking outlined by the Basel Committee on Banking Supervisions ("The Basel Committee"), in the papers: "*Risk Management Principles for E-banking"*[2] and "*Management and Supervision of Cross-Border E-banking Activities*"[2] issued in July 2003.

The Bank encourages credit institutions to read and understand the principles set forth in the abovementioned documents and to continuously monitor updated publications related to e-banking activities posted on among other places on The Basel Committee's website[3].

[1] See appendix 1 for definition.
[2] http://www.bis.org/publ/bcbs98.htm and http://www.bis.org/publ/bcbs99.htm
[3] http://www.bis.org/

## II. Legal base and scope

These Provisions and Guidelines are issued pursuant to article 2, paragraph 2 of the National Ordinance on the Supervision of Banking and Credit Institutions 1994 (N.G. 1994, no. 4).

The Provisions and Guidelines apply to all credit institutions that conduct e-banking activities in and/or from the islands of Curaçao and Sint Maarten and are licensed pursuant to the aforementioned National Ordinance. These institutions are hereafter referred to as "credit institutions".

# III. Implementation

To ensure a high standard of e-banking risk management on the islands of Curaçao and Sint Maarten, credit institutions are required to have implemented the "**Provisions and Guidelines for Safe and Sound Electronic Banking"** by the end of 2007.

The Bank recognizes that each credit institution's risk profile is different and will require:

1. a risk mitigation approach appropriate for the scale of the e-banking operations;
2. the materiality of the risk present; and
3. the true ability of the credit institution to manage these risks.

These differences imply that the risk management principles and recommendations presented and referred to in these Provisions and Guidelines are intended to be flexible enough to be implemented. However, each credit institution is required to implement a minimum of risk mitigating counter measures. The minimum required measures are stated in chapters VII, VIII, IX and X.

The Bank will verify the implementation of the Provisions and Guidelines during its offsite and onsite supervisions. Based on these examinations and its offsite reviews, the Bank will determine the adequacy of the credit institutions' risk management of e-banking. The Bank also may implement other monitoring processes to facilitate its ongoing supervision of e-banking.

# IV. Supervisory approach

The Bank's supervisory objective is to establish and maintain a safe and sound environment for the development of e-banking activities in and/or from the islands of Curaçao and Sint Maarten.

The general principle is that credit institutions are expected to implement the relevant risk management controls that are "fit for purpose", i.e., commensurate with the risks associated with the types, complexity, and amounts of transactions allowed, the electronic delivery channels adopted, and the risk management systems of individual credit institutions.

In developing these Provisions and Guidelines, the Bank has considered the supervisory approach and guidance by the Basel Committee in particular and those of other regulatory communities. The Bank emphasizes that these Provisions and Guidelines are not intended to prescribe uniform or all-inclusive principles and practices in managing the risks for all kinds of e-banking activities. The minimum required measures are stated in chapters VII, VIII, IX and X.

Credit institutions should take into account all relevant laws and provisions, policies, and guidelines issued by the Bank. They include but are not limited to:

- The National Ordinance on Identification of Clients when rendering Financial Services (N.G. 1996, no.23);
- The National Ordinance on Reporting of Unusual Transactions (NG.1996, no21);
- National Ordinance on Foreign Exchange Traffic (N.G. 1981, no.67);
- The BNA Corporate Governance Summary of Best Practice Guidelines;
- The BNA Provisions and Guidelines regarding Detection and Deterrence of Money Laundering and Terrorist Financing for Credit Institutions; and
- The BNA Policy rule for Sound Business Operations in the Event of Incidents and Integrity-Sensitive Positions.

The Bank may prescribe new rules and regulations to administer and carry out the purposes of this regulation, including rules and regulations to define or further define terms used in this regulation and to establish limits ore requirements other than those specified in this regulation.

The Bank reserves the right, in individual cases of (partially) non-compliance, to impose conditions or initiate consultations on a limitation of the e-banking activities.

# V. Risk Management

The Board of Supervisory Directors (hereafter "the Supervisory Board") and senior management of credit institutions are responsible for managing the institution's risks. Its risk profile will become more complex if the institution provides e-banking transactions. Therefore, the Supervisory Board and senior management should be well involved in the development of the institution's e-banking business strategy and ensure that the risk characteristics are fully understood and operational and that security dimensions of the electronic activities are appropriately considered and addressed.

To mitigate the risks associated with all e-banking activities, credit institutions should have in place a comprehensive risk management process that assesses risks, controls risk exposure, and monitors risks. This comprehensive risk management framework should be integrated into the credit institutions' overall risk management framework. The risk management process should be supported by appropriate oversight by the Supervisory Board and senior management or its designated committee. The process should be carried out by adequate staff with the necessary knowledge and skills to deal with the technical complexities of e-banking. As a result, the applicable risk management policies and processes and the relevant internal controls and audits should be enforced as required in the credit institutions risk management systems, and carried out as appropriate for the credit institution's e-banking services.

*Credit institutions should implement at least the minimum required risk mitigating countermeasures as stated in chapters VII, VIII, IX, and X. However, to achieve a comprehensive risk management control regarding e-banking services, credit institutions should always take into account the 14 risk management principles for e-banking activities[4] outlined by the Basel Committee.*

These Provisions and Guidelines focus on the risks and risk management techniques associated with internet delivery channels. The principles are applicable to all forms of e-banking activities.

[4] The 14 risk management principles and recommendations for e-banking activities are explained in the document "Risk Management Principles for E-banking" available at: http://www.bis.org/publ/bcbs98.htm

# VI. E-banking related risks

E-banking does not open up new risk categories, but rather increases and modifies existing risks and creates new risk management challenges. Because of rapid changes in information technology, no description of such risk categories can be exhaustive. However, the Bank has identified below a number of risks specifically associated with e-banking for bank supervision purposes. The board of supervisory directors and senior management must recognize these risks and should ensure that the risk management controls and systems have been reviewed and modified where necessary to address specific risk management challenges associated with e-banking.

**Strategic risk**

This is the current and prospective risk arising from amongst other things, from adverse business decisions or improper implementation of decisions. Senior management must fully understand the strategic and technical aspects of e-banking. Spurred by competitive and peer pressures, credit institutions may seek to introduce or expand e-banking activities without an adequate cost-benefit analysis. In managing the strategic risk associated with e-banking services, credit institutions should develop clearly defined e-banking objectives by which the institution can evaluate the success of its e-banking strategy.

**Transaction/operations risk**

This is the current and prospective risk arising from among other things fraud, processing errors, systems descriptions negligence, and the inability to maintain expected service levels. It includes failure of communications, breakdown of data transport or processing, internal control system deficiencies, and management failure. Offering innovative services that have not been standardized increases the complexity of an institution's activities and the quantity of this risk. A high level of transaction/operations risk may exist with e-banking products, because of the need to have sophisticated internal controls and constant availability. The level of transaction/operations risk is affected by the structure of the institution's processing environment, including the types of services offered and the complexity of the processes and supporting technology. Credit institutions should make certain that customers who transact on the internet cannot later deny having originated the transactions. Third-party providers also increase transaction/operations risks, since the credit institutions do not have full control over a third party. Without seamless process and system connections between the bank and the third party, there is a higher risk of transaction errors. The key to controlling transaction/operations risk lies in adapting effective policies, procedures, and controls to meet the risk exposures introduced by e-banking. Basic internal controls such as segregation of duties and dual controls remain important. Credit institutions should determine the appropriate level of security controls based on their assessment of the sensitivity of the information to the customer and to the institution and on the institution's established risk tolerance level.

**Compliance/legal risk**

This is the failure to comply with statutory or regulatory obligations or contractual agreements such as laws, rules and regulations and the violation of ethical standards. Compliance/legal risk may lead to diminished reputation, reduced business opportunities, and actual monetary losses. Conflicting laws, tax procedures, and reporting requirements

across different jurisdictions add to the risk. The need is to keep customer data private and to seek customers' consent before sharing the data, unless allowed otherwise by law, such as the reporting to the FIU/MOT (Meldpunt Ongebruikelijke Transacties). FIU also adds to compliance/legal risk. Credit institutions need to understand and interpret existing laws, regulations, and ethical standards that apply to e-banking and ensure consistency with other channels such as branch banking.

**Reputation risk**
This is the current and prospective risk arising from negative publicity regarding the credit institution's business. A bank's reputation can be damaged by e-banking services that are poorly executed (e.g., limited availability, buggy software, poor response, the use of inadequate point of sale devices). To meet customers' expectations, credit institutions should have effective capacity, business continuity, and contingency planning. Credit institutions should also develop appropriate incident response plans, including communication strategies, which ensure business continuity, control reputation risk, and limit liability associated with disruptions in their e-banking services.

**Information security risk**
Information security includes protecting information and/or information systems from unauthorized access, use, disclosure, disruption, modification, or destruction, to provide integrity, confidentiality, and availability. Information security risk arises out of lax information security processes', and may expose the institution to malicious hacker or insider attacks, viruses, denial-of-service attacks, data theft, data destruction and fraud. The speed of change of technology and the universal accessibility of the internet channel makes this risk especially critical.

**Contingency/technological risk**
Contingency/technological risks are risks related to any adverse outcome, damage, loss, disruption, violation, irregularity, or failure arising from the use of or reliance on computer hardware, software, electronic devices, and online networks and telecommunications systems. These risks can also be associated with among other things application security, systems failures, processing errors, software defects, operating mistakes, hardware breakdowns, capacity inadequacies, network vulnerabilities, control weaknesses, security shortcomings, malicious attacks, hacking incidents, fraudulent actions, and inadequate recovery capabilities.

# VII. Risk mitigating counter measures

The risk management controls and policies related to e-banking should cover, at a minimum, the following risk mitigating countermeasures:

**Authentication of customers**
Credit institutions should select reliable and effective authentication techniques to validate the identity and authority of their e-banking customers. Single-factor authentication[5], as the only control mechanism, is insufficient and not accepted by the Bank for transactions involving access to customer information or the movement of funds to other parties. Authentication methods that depend on more than one factor are more difficult to compromise than single-factor methods. Consequently, multifactor authentication[6] methods (such as two-factor authentication[7]) are more reliable and provide stronger assurance in authentication. Credit institutions should ensure that customers are verified and their identities established before conducting business over the internet. Password generating devices, biometric methods, challenge-response systems, and public key infrastructure are some ways of strengthening the authentication process, as indicated in our letter of July 27, 2006, with reference CE/nl/2006-10.581.

Current examples of the proper use of multi-factor authentication are:

- Internet banking websites using a user id and password in combination with a token device to connect to the on-line banking application;
- POS at the supermarket requires an ATM card and a pin code for access and authentication before completing a transaction; and
- ATM machines require an ATM card and a pin code for access and authentication before collecting money from the ATM machine.

Current examples of the improper use of access and authentication are:

- Internet banking websites using only a user id and password to connect to the on-line banking application; and
- POS machines at gasoline stations allowing only an ATM card input to complete a transaction to fill up the fuel tank.

Credit institutions are required to use multi-factor authentication for internet banking:

- When the user logs on to the banking system; and
- When the user wants to make a transaction.

[5] Single-factor authentication involves the use of one factor to verify customer identity, namely user id and password.
[6] Multifactor authentication utilizes two or more factors to verify customer identity.
[7] Two-factor authentication involves the use of two factors, e.g., a password-generating device along with the user id/password, ATM card and pin code, user id/password and token device.

**Confidentiality and integrity of information**
E-banking services entail transmission of sensitive information over the internet and credit institution's internal networks. Therefore, credit institutions should therefore implement appropriate technologies to maintain confidentiality and integrity of sensitive information while it is being transmitted over the internal and external networks and also when it is stored inside database systems. The use of cryptographic technologies is required to protect the confidentiality of sensitive information. Credit institutions should choose cryptographic technologies appropriate to the sensitivity and importance of information and the extent of protection needed. They must ensure that all intelligent electronic devices that capture information do not expose/store information such as the PIN number or other information classified as confidential and must also ensure that a customer's PIN number cannot be printed for any reason whatsoever. In addition, credit institutions must provide safe- to- use intelligent electronic devices and ensure that customers are able to make safe use of these devises at all times.

**Application security**
Inadequate application security in e-banking systems increases the risk of intruders exploiting the system. Credit institutions should ensure an appropriate level of application security in their e-banking systems. When credit institutions select system development tools or programming languages for developing e-banking application systems, they should evaluate the security features that can be provided by different tools or languages to ensure that effective application security can be implemented. In the case of selecting an e-banking system developed by a third party, credit institutions should take into account the appropriateness of the application security of the system. Credit institutions are required to test new or enhanced applications thoroughly using a general accepted test methodology in a test environment.

E-Banking applications should protect against common techniques that fraudsters use to break into the credit institution's server by misleading its application.
E.g.:

- SQL injection;
- cookie poisoning/tempering;
- cross site scripting; and
- entering programming code into fields that lack input validation.

Credit institutions should make reasonable effort to ensure non-repudiation of e-banking transactions using strong authentication mechanisms and application security.

**Internet infrastructure and security monitoring**
Credit institutions should establish an appropriate operating environment that supports and protects their e-banking systems. Credit institutions should proactively monitor their e-banking systems and internet infrastructure on an ongoing basis to detect and record any security breaches, suspected intrusions, or weaknesses. Credit institutions should ensure that adequate controls are in place to detect and protect against unauthorized access to all critical e-banking systems, servers, databases, and applications.

This includes, but is not limited by:

- A formal[8] information security policy;
- A formal server security policy;
- A formal physical security policy;
- A formal disaster recovery plan;
- A formal backup and recovery procedure;
- A formal change management procedure;
- A formal patch management procedure;
- A formal security monitoring procedure;
- A formal virus update procedure;
- Placement of external accessible servers placed in a De-militarized zone (DMZ);and
- Protecting critical hosts with intrusion detection systems.

**Outsourcing**

Credit institutions may rely on an outside service provider to operate and maintain IT systems or business processes that support their e-banking services. In such cases, credit institutions should exercise appropriate due diligence in evaluating their reputation, credit status, and viability. Credit institutions must ensure that the service providers and vendors can perform as promised and that they are capable of keeping abreast of new or changing technology. When contracting for e-banking services, credit institutions must carefully consider how they intend to use third parties to design, implement, and support all or part of their e-banking systems. A credit institution's contracts with technology providers should ensure that the provided activities match applicable legal and policy standards. Credit institutions should maintain control through a Service Level Agreement over the services and products provided by third parties and ensure that the outsourced service is subject to independent assessment and the customer data are kept confidential.

A global development is buying through telephone services. Credit institutions rely on the telecommunication businesses (e.g., UTS) to handle part of the transaction between the retail business and the credit institution or the consumer and the credit institution. Credit institutions are responsible for adequately controlling these new types of payment services and should take into account abovementioned risk mitigating countermeasures.

[8] Formal means "in writing and approved by management"

**Internet banking**
Credit institutions should put in place procedures for maintaining the credit institution's web site, which should ensure at least the following:

1. Only authorized staff should be allowed to update or change information on the web site;
2. Updates of critical information (e.g., interest rates) should be subject to dual verification;
3. Web site information and links to other websites should be verified for accuracy and functionality;
4. Management should implement procedures to verify the accuracy and content of any financial planning software, calculators, and other interactive programs available to customers on an internet websites or other e-banking service;
5. Links to external web sites should include a disclaimer that the customer is leaving the financial institution's site and provide appropriate disclosures, such as noting the extent, if any, of the bank's liability for transactions or information provided at other sites;
6. Credit institutions must ensure that the Internet Service Provider (ISP) has implemented a firewall to protect the financial institution's website where outsourced;
7. Credit institutions should ensure that installed firewalls are properly configured and institute procedures for continued monitoring and maintenance arrangements are in place; and
8. Credit institutions should ensure that summary-level reports showing website usage, transaction volume, system problem logs, and transaction exception reports are made available to the institution by the web administrator.

## VIII. Internal control

The risk management controls and policies related to e-banking should also cover, at a minimum, the following risk mitigating countermeasures:

**Segregation of duties**

As in any traditional process, segregation of duties is a basic internal control measure designed to reduce the risk of fraud in operational processes and systems. The credit institution's management must identify and mitigate areas where conflicting duties create the opportunity for insiders to commit fraud. Credit institutions should ensure that appropriate measures are taken to protect the data integrity of e-banking transactions, records, and information. No one employee should be able to process a transaction from start to finish.

**Recordkeeping**

All e-banking transactions should generate clear audit trails, which should be archived and kept for 10 years. ATM video surveillance recordings should be archived for at least one year. It is also vital to generate and protect records of customer instructions in a legally acceptable format. Credit institutions should strengthen information security controls to preserve the confidentiality and integrity of customer data. Firewalls, ethical hacking tests, physical and logical access controls are some of the methods available. Recordkeeping requirements should be based upon the level of activity and risk.

**Dual controls**

Some sensitive transactions necessitate making more than one employee approve the transaction before authorizing the transaction. Large electronic funds transfers or accesses to encryption keys are examples of two e-banking activities that should warrant dual controls.

**Reconcilements**

E-banking systems should provide sufficient accounting reports to allow employees to reconcile individual transactions to daily transaction totals.

**Monitor suspicious activity**

Credit institutions should establish fraud detection controls that could prompt additional checking of suspicious activity. Some potential concerns to consider include false or erroneous application information, large check deposits on new e-banking accounts, unusual volume or size of funds transfers, multiple new accounts with similar account information or originating from the same internet address, and unusual account activity initiated from a foreign internet address.

**Incident response**

Credit institutions should put in place formal incident response and management procedures for timely reporting and handling of suspected or actual security breaches, fraud, or service interruptions of their e-banking services. The incident response and management procedures should allow credit institutions to quickly identify the origin of the weakness and contain the damage and assess the potential scale and impact of the incident. Credit institutions should also identify and notify affected customers and collect and preserve forensic evidence as appropriate to facilitate the subsequent investigation and potential prosecution of suspects

and intruders. Furthermore, the incident response procedures should include strategies for dealing with adverse media and customer reactions in a timely way. In the event of an incident as described above, the credit institutions should notify the Bank immediately.

**Error checks**
E-banking activities provide limited opportunities for customers to ask questions or clarify their intentions regarding a specific transaction. Institutions can reduce customer confusion and the potential for unintended transactions by requiring written contracts explaining rights and responsibilities, by providing clear disclosures and on-line instructions or help functions, and by incorporating proactive confirmations into the transaction initiation process. On-line instructions help features and proactive confirmations are typically part of the basic design of an e-banking system and should be evaluated as part of the initial due diligence process. On-line forms can include error checks to identify common mistakes in various fields. Proactive confirmations can require customers to confirm their actions before the transaction is accepted for processing. For example, a bill payment customer would enter the amount and date of payment and specify the intended recipient. But, before accepting the customer's instructions for processing, the system might require the customer to review the instructions entered and then confirm the instruction's accuracy by clicking on a specific box or link.

**Alternate channel confirmations**
Credit institutions should consider the need to have customers confirm sensitive transactions like enrollment in a new on-line service, large funds transfers, account maintenance changes, or suspicious account activity. Positive confirmations for sensitive on-line transactions provide the customer with the opportunity to help catch fraudulent activity. Financial institutions can encourage customer participation in fraud detection and increase customer confidence by sending confirmations of certain high-risk activities through additional communication channels such as the telephone, e-mail, or traditional mail.

**Customer data protection**
Misuse or unauthorized disclosure of confidential customer data may expose a financial institution to customer litigation. The general requirements and controls that apply to paper-based transactions also apply to electronic financial services. To meet expectations regarding the privacy of customer information, credit institutions should ensure that their privacy policies and standards comply with existing applicable regulations.

Furthermore, credit institutions should at least:

1. ensure the security and confidentiality of customer records and information;
2. protect customers against any anticipated threats or hazards to the security or integrity of such records; and
3. protect customers against unauthorized access to or use of such records or information that could result in substantial harm or inconvenience to any customer.

## IX. Cross-border e-banking activities

Before engaging in cross-border e-banking transactions, credit institutions should ensure that adequate information is disclosed on their websites to allow potential customers to make a determination of the credit institution's identity, home country, and whether it has the relevant regulatory license(s) before they establish the business relationship. This information will improve transparency and minimize legal and reputation risk associated with cross-border e-banking activities. By engaging in cross-border e-banking activities, credit institutions should ensure that they are complying with the Provisions and Guidelines regarding Detection and Deterrence of Money Laundering and Terrorist Financing and Foreign Exchange Regulations.

To achieve a comprehensive risk management control policy for cross-border e-banking, credit institutions should, in addition to implementing the 14 risk management principles for e-banking activities, also implement, where necessary, the 2 principles and recommendations for cross-border e-banking activities[9] outlined by the Basel Committee.

[9] The principles and recommendations for cross-border e-banking activities can be found on the BIS website at http://www.bis.org/publ/bcbs99.htm

# X. Customer security, education, and transparency

An important aspect of customer security and risk management is customer education. Therefore, credit institutions should pay special attention to the provision of easy-to-understand and prominent advice to their customers on e-banking security precautions.

At a minimum security precautionary advice for customers should cover the following issues:

- Password and user ID selection and protection, e.g., not to select passwords incorporating such info as birthday and to avoid using the same password for accessing other online services;
- Not to disclose their personal information to unauthorized persons or to any doubtful websites;
- Never to write down their PIN number;
- To cover their hands when typing at POS systems;
- To be aware of phishing e-mails; and
- To ensure that their pc's are securely configured and adequately protected from malicious programs and viruses, e.g., regularly updating their anti-virus software.

Credit institutions should use effective methods and channels to communicate with customers on security precautions. Such channels can include websites and messages printed on customer statements.

**Fee disclosure**
Automated Teller Machine (ATM) and Point of Sale (POS) operators who impose a fee on consumer for providing host transfer services should notify the consumer in advance that a fee is imposed for providing the service and the amount of any such fee.
The notification should be placed in a prominent and conspicuous location on or at the ATM and/or the POS where the consumer initiates the electronic fund transfer.

## **Appendix 1:** Glossary/Definitions

**Authentication**
The techniques, procedures, and processes used to verify the identity and authorization of prospective and established customers.

**Board of Supervisory Directors**
The governing body of an institution, elected by the shareholders, to oversee and supervise the management of the institution's resources and activities. This body is ultimately responsible for the conduct of the institution's affairs, and controlling its direction and, hence, it's overall policy.

**Cross-border e-banking activities**
The provision of transactional on-line banking products or services by a bank in one country to residents of another country**.**

**E-banking**
The automated delivery of new and traditional banking products and services directly to customers through electronic and interactive communication channels. E-banking includes the set up, maintenance, internal control, and other aspects of the systems that will enable credit institution customers and/or other persons to access accounts, transact business, or obtain information on financial products and services through the above channels and a private or public network, including the internet. Customers access e-banking services using an intelligent electronic device, such as a personal computer (PC), personal digital assistant (PDA), automated teller machine (ATM), point of sale devices (POS), Kiosk, or Touch Tone telephone.

**Identification**
The procedures, techniques, and processes used to establish the identity of a customer when opening an account.

**Meldpunt Ongebruikelijke Transacties (MOT/FIU)**
Pursuant to article 11 of the National Ordinance on the reporting of Unusual Transactions (N.G. 1996, no. 21), any (legal) person who provides a financial service is obliged to inform the MOT "Meldpunt Ongebruikelijke Transacties" of an unusual transaction that is contemplated or has taken place.

**Risk management**
The ongoing process of identifying, measuring, monitoring, and managing potential risk exposures.

**Senior management**
Comprises the individuals entrusted with the daily management of the operations to achieve the institution's objectives.