Document Type: *Policy*

Whistleblowing Policy

Competent Structure: Internal Audit Department

Date: January 2023

Version 6

SUMMARY

Document Type:	Policy	
Structure Responsible for the Document:	Internal Audit Department	
Contacts	Head of Internal Audit Department: Fabio Marchesi fabio.marchesi@illimity.com	
Structures Involved in the Process of Sharing the Present Version	Compliance & AFC Officer ; HR & Organization	
Recipients of the Regulation	**Parent Company**	**Other Companies**
	illimity Bank S.p.A.	
Version approved by:	Chief Executive Officer	
Date of approval	26/01/2023	
Date of validity	27/01/2023	

VERSIONS

Name of regulation and version	Main changes	Approving body and date
Whistleblowing Policy V.1	Drafting of the Document	Board of Directors, 17 December 2018
Whistleblowing Policy V.2	Amendment of the policy previously in force in the Bank, which required a detailed revision in light of the changes in key external and internal regulations as well as the Bank's renewed organisational and business structure	Board of Directors, 18 April 2019
Whistleblowing Policy V.3	Amendment of the policy previously in force in the Bank in order to include the new physical reporting channel ("letter box") and make certain changes of a formal nature	Chief Executive Officer , 4 February 2020
Whistleblowing Policy V.4	Updating of the document incorporating the new ICT tool for reporting breaches (@Whistleblowing)	Chief Executive Officer, 23 September 2020
Whistleblowing Policy V.5	Renaming of the document and updating of the definition of "reporting" in order to include parties outside the Bank	Chief Executive Officer, 17 December 2021
Whistleblowing Policy V.6	Updating of the document renaming the "Corporate Body with a control function" and providing timeframes within which to deliver feedback to the reporting person	Chief Executive Officer, 26 January 2023

illimity
BANCA OLTRE LA FORMA

Contents

1 PURPOSE

The aim of this Policy is to determine the aspects of a legislative, regulatory, procedural and organisational nature of the whistleblowing system that the Group intends to govern in accordance with the regulatory provisions of reference, detailed in paragraph 3 below.

This Policy also constitutes an implementation of the requirements of Legislative Decree no. 231/2001 (at paragraphs 2-bis, 2-ter and 2-quarter of article 6) on reporting to the Supervisory Body.

2 GLOSSARY

Abbreviations	
ABI	Italian Banking Association
CRD	Capital Requirements Directive
TUB	Consolidated Law on Banking
TUF	Consolidated Law on Finance

Definitions	
ORGANISATIONAL STRUCTURES (OR STRUCTURES)	The types of organisational structure of which illimity's Organisation Chart is composed in which the detailed responsibilities are assigned as described in the "Organisational Structure Regulation".
PERSONNEL	Pursuant to article 1, paragraph 1h-novies of the TUB, "personnel" shall mean "employees and those persons who in any case operate on the basis of relations that determine inclusion in the business organisation, also by a means other than a permanent employment contract".
RETALIATION	Action designed to deter the submission of a report. By way of example, the following are forms of retaliation: • dismissal or suspension; • demotion or withholding of promotion; • transfer of duties; change of location; reduction in wages; change in working hours; • withholding of training; • imposition or administering of any disciplinary measure, reprimand or other penalty, including financial penalty; • coercion, intimidation, harassment or ostracism; • failure to renew or early termination of a temporary employment contract; • discrimination, disadvantageous or unfair treatment.
REPORTED PERSON	Person to whom the whistleblowing breaches refer.

REPORTING PERSON	Person reporting a breach who belongs to one of the following categories: • employees of illimity Bank S.p.A. and those persons operating on the basis of relations that determine inclusion in the business organisation, also by a means other than a permanent employment contract; • members of the corporate bodies of illimity Bank S.p.A.; • employees of other Group companies and those operating on the basis of relations that determine inclusion in the business organisation of these companies; • any other person external to the Bank.
WHISTLEBLOWING	A communication made by a reporting person concerning actions or facts relating to: • breaches of internal or external regulations that govern the activity of illimity Bank S.p.A. or other Group companies, including the principles and rules of conduct contained in the Code of Ethics; • illegal or fraudulent conduct carried out by employees, members of the corporate bodies or third parties (suppliers, consultants, collaborators, financial promoters or Group companies) that may, directly or indirectly, cause damage to the Group's results or net assets and/or to its image.

3 LEGISLATIVE AND REGULATORY REFERENCES

Legislative Decree no. 72 of 12 May 2015 and subsequent amendments incorporates into Italian legislation the CRD IV Directive[1] as regards access to the activity of credit institutions and the prudential supervision of credit institutions and investment firms, thereby making changes to the TUB[2] and the TUF[3].

In particular, this decree sets up systems for reporting breaches to banks and other qualified parties, to the Bank of Italy and to Consob.

Regarding the area of employee protection, reference should be made to the provisions and guarantees set forth in Law no. 300/1970 (the Employees Charter) and corporate disciplinary codes.

European Delegation Law 2014[4] requires the government to:

- regulate the means of reporting, within intermediaries and towards supervisory authorities, breaches of the discipline on the MIFID II and MIFIR[5], financial instruments markets, also taking into account the profiles of confidentiality and protection of the persons involved, providing for possible measures to encourage reporting useful for the purpose of exercising supervisory activity and extending the possible means of also reporting other breaches;
- implement the provisions of Regulation (EU) No. 596/2014 on market abuse, pursuant to which financial intermediaries are required to have appropriate internal procedures in place for their employees to report breaches regarding market abuse. The detailed legislation must govern whether the reporting is to be made directly to the competent authority or Consob.

Legislative Decree no. 90 of 25 May 2017 transcribes the Fourth Anti-Money Laundering Directive[6] into Italian

[1] Namely Directive 2013/36/EU amending Directive 2002/87/EC and repealing Directives 2006/48/EC and 2006/49/EC.
[2] Cf. Legislative Decree no. 385 of 1 September 1993, with particular reference to article 52-bis.
[3] Cf. Legislative Decree no. 58 of 24 February 1998, with particular reference to article 4-undecies.
[4] Official Journal no. 176 of del 31 July 2015.
[5] Directive 2014/65/EU and Regulation (EU) No.600/2014 respectively.
[6] Directive (EU) 2015/849.

law and among its provisions is the need to introduce whistleblowing systems that require obliged entities to adopt procedures for employees or persons in a comparable position to report potential or actual breaches of money laundering prevention and terrorist financing provisions.

Regarding the detailed discipline, in respect of internal reporting on the possibility that unlawful acts have been committed, Law no. 179 of 30 November 2017 on "Provisions for the protection of persons reporting criminal offences or irregularities of which they have become aware as part of a public or private employment relationship" has been issued, this extending the provisions of article 6, paragraph 2-bis et seq. of Legislative Decree no. 231/2001; in addition, on the same subject, reference should be made to Consob Resolution no. 20249 of 28 December 2017[7].

Concerning the role of the corporate bodies connected with the situations of whistleblowing procedures reference should also be made to the ABI Guidelines of 28 October 2015 on "Detailed analyses for setting up an internal whistleblowing system".

As far as the Administrative Responsibility of Legal Persons is concerned, it should be noted that Law no. 179 of 30 November 2017 on "Provisions for the protection of persons reporting criminal offences or irregularities of which they have become aware as part of a public or private employment relationship" has added three new paragraphs to article 6 of Legislative Decree no. 231/2001, designed in fact to regulate whistleblowing.

More specifically, an entity's Organisation Model must provide for one or more channels that enable everyone operating in the interest of the entity (whether at a top or subordinated level) to submit, as protection of the integrity of the entity itself, a detailed report on unlawful conduct relevant pursuant to Legislative Decree no. 231/2001 based on precise and concordant factual items or breaches of the Organisation Model adopted by the entity of which they have become aware when performing their duties.

4 SCOPE OF APPLICATION

This Policy, concerning the internal system for reporting breaches, is applicable to all Group companies, which must incorporate the provisions of this Policy into their internal rules and regulations and make an appropriate distribution of these provisions to all of their staff.

4.1 Objective scope of application

Pursuant to article 52-bis, paragraph 1 of the TUB, reporting regards any action or fact that constitutes a breach of the laws and regulations governing banking activity – meaning by this the activity governed by article 10, paragraphs 1, 2 and 3 of the TUB – as well as any suspicion that another breach regarding activities for collecting savings (such as for example the sale of banking products and services) or extending credit (such as for example the granting of loans or endorsement credit) has occurred or may occur, or any breach relating to activities connected with or instrumental to banking activities (such as for example the acquisition of equity investments).

A number of examples (not comprehensive) of areas to which said laws and regulations relate, which are accordingly susceptible to reporting, are set below in order to provide practical details of the scope of application of this Policy:

- breaches of internal and external regulations that govern the activity of illimity Bank S.p.A. or other Group companies, including those contained in the Bank's Organisation, Management and Control Model, as well as the principles and rules of conduct contained in its Code of Ethics;
- unlawful or fraudulent conduct, carried out by employees, members of the corporate bodies or third parties (suppliers, consultants, collaborators, financial promoters or Group companies) that may, directly or indirectly, cause damage to the Group's results or net assets and/or to its image;
- criminal offences committed by employees, members of the corporate bodies or third parties (suppliers, consultants, collaborators, financial promoters or Group companies) to the detriment of the Bank or which may lead to a liability for the Bank;
- any conduct that gives rise to conflicts of interest, adopted without full compliance with the rules and procedures of control envisaged for such situations (such as for example the conflict of interest of an employee in a lending transaction in which he or she has a personal interest).

[7] Regulation on provisions implementing Legislative Decree no. 58 of 24 February 1998 on market matters (article 60-bis).

Any reporting based on interpersonal questions which follows the traditional channels (for example line supervisor, the human resources function) is excluded from the admissible cases.

The Bank is also free to extend the procedure to reporting that regards the breach of internal norms, procedures and regulations other than those governing banking activity, given that the reporting and relative procedure for dealing with this do not fall within the sphere of article 52-bis of the TUB; the Bank will provide information to the employees on the fact that, in this situation, they cannot benefit from the same prerogatives as those provided by the law (right to confidentiality of the identity of the reporting person, rights of the reported person, etc.).

In addition, pursuant to Legislative Decree no. 231/2001, reporting must regard unlawful conduct or breaches of the Bank's Organisation Management and Control Model that are detailed and based on precise and concordant items.

4.2 Subjective scope of application

Reports may be made by the Bank's staff, members of the corporate bodies, members of the staff of other Group companies and any other person outside the Bank.

5 THE ROLE OF THE CORPORATE BODIES AND STRUCTURES INVOLVED

5.1 The corporate body responsible for strategic supervision

In line with the provisions of the ABI Guidelines of 28 October 2015, the corporate body responsible for strategic supervision:

- establishes and approves the internal system designed to enable actions and facts that may constitute a breach of the norms governing banking activity to be reported;
- after obtaining the opinion of the corporate body responsible for control, appoints the Head of the internal system for reporting breaches;
- after obtaining the opinion of the corporate body responsible for control, receives and approves the annual report containing aggregate information on the results of the work performed by the Head of the internal system for reporting breaches as a consequence of the reporting received;
- encourages the use of internal reporting systems and fosters the dissemination of a legality culture by delegating the Head of the internal system for reporting breaches to arrange training and the provision of information for personnel.

5.2 The corporate body with a control function

In line with the provisions of the ABI Guidelines of 28 October 2015, the corporate body with a control function:

- oversees the proper functioning of the internal system for reporting breaches;
- obtains periodic information from the Head of the internal system for reporting breaches on any reporting of breaches received;
- expresses its opinion to the corporate body responsible for strategic supervision on the appointment of the Head of the internal system for reporting breaches;
- expresses its opinion to the corporate body responsible for strategic supervision on the annual report containing aggregate information on the results of the work performed by the Head of the internal system for reporting breaches as a consequence of the reporting received.

5.3 Head of the internal system for reporting breaches

The Head of the internal system for reporting breaches[8] (hereinafter also the "Head of Whistleblowing") is appointed by the body with a strategic supervision function on the basis of the following characteristics:

- he is not hierarchically or functionally subordinate and accordingly reports directly to the corporate bodies[9];
- he does not perform operational duties;
- he does not participate in the adoption of any decision-making provisions resulting from the reported breaches, which are remitted to the competent corporate functions or bodies[10].

The Head of the internal system for reporting breaches [11]:

- examines and assesses the reports of breaches received;
- ensures the procedure for reporting breaches has been correctly followed;
- where relevant reports the information reported to the corporate bodies directly and without delay;
- guarantees the confidentiality of the information received;
- ensures the confidentiality of the reporting person and the person alleged to be responsible for the breach, without prejudice to the rules governing investigations or proceedings initiated by the judicial authorities in relation to the facts to which the reporting relates;
- provides suitable protection for the reporting person against retaliatory, discriminatory or in any case unfair conduct as a result of the reporting;
- in accordance with legislation on personal data protection draws up an annual report on the proper functioning of the internal reporting system containing aggregate information on the results of the work performed as a consequence of the reporting received, which is approved by the corporate bodies and made available to the Bank's staff;
- tales care of the training of the Bank's staff, describing in a clear, precise and complete manner the internal procedure for reporting adopted, indicating the controls put in place to ensure the confidentiality of the reporting person's personal data and those of the person alleged to be responsible for the breach, with the express notice that the provision of article 15 of Regulation (EU) 2016/679 of the European Parliament and of the Council regarding the identity of the reporting person is not applicable and that this can only be revealed with their consent and when the knowledge is essential for defending the reported person[12].

  The reported person must in any case be informed with a reasoned communication – unless the communication may jeopardise the purpose of the limitation – that the exercising of his rights may, in any case, be delayed, restricted or excluded for the time period and to the extent that this constitutes a necessary and proportionate measure, given his basic rights and legitimate interests, in order to safeguard the interests of the reporting person and the investigation procedure itself;
- looks after the maintenance of the ICT reporting tool (called "@Whistleblowing") provided by BDO Italia S.p.A. and on a regular basis checks that it continues to function properly.

[8] As set forth in the ABI's Guidelines of 28 October 2015, this person must be included in the corporate structure as head of a function set up ad hoc, or else chosen from the figures in charge of the control functions such as the Compliance structure or the Internal Audit structure.
[9] Regulation on provisions implementing Legislative Decree no. 58 of 24 February 1998 on market matters (article 60-bis) (adopted by Consob by way of Resolution no. 20249 of 28 December 2017); ABI Guidelines 2015.
[10] Regulation on provisions implementing Legislative Decree no. 58 of 24 February 1998 on market matters (article 60-bis) (adopted by Consob by way of Resolution no. 20249 of 28 December 2017).
[11] Circular no. 285 of 17 December 2031 "Supervisory provisions for banks", Part I, Title IV, Chapter 3, Section VIII.

[12]Circular no. 285 of 17 December 2013, "Supervisory provisions for banks", Part I, Title IV, Chapter 3, Section VIII; Regulation on provisions implementing Legislative Decree no. 58 of 24 February 1998 on market matters (article 60-bis) (adopted by Consob by way of Resolution no. 20249 del 28 December2017); article 52-bis of the TUB.

5.4 Other persons involved

The Building Manager prepares the letter box at the Bank's premises and hands over its keys to the Chairman of the corporate body with a control function.

6 PROCEDURE FOR REPORTING BREACHES

The person reporting the alleged breach must forward his report – either anonymously or bearing his name – by the following means:

- using the ICT tool @Whistleblowing (accessible via web at the address **https://digitalroom.bdo.it/illimitybank**), through which he receives an immediately confirmation of report's receipt and a unique code required for monitoring the state of progress of the report processing. The Head of Whistleblowing views the reports received on the dashboard included in the tool to which the members of Audit and Internal Control Committee and Supervisory Body of the reporting person's reference company have access (in reading mode only). If the report regards the Head of Whistleblowing, an "alternative" operating process is envisaged under which the report is visible (in reading/writing mode) to the Chairman of the Audit and Internal Control Committee and (in reading mode only) to the other members of the Committee as well as to the members of the Supervisory Body. In this case, the activities for which the Head of Whistleblowing is usually responsible must be performed by the Chairman of the Audit and Internal Control Committee ;
- by way of the letter box placed in the company's premises, whose access keys are held by the Chairman of the Audit and Internal Control Committee. In this case the chairman of the corporate body with a control function immediately informs the Head of Whistleblowing and the Supervisory Body that the report has been received, dragging it into a suitable section of the ICT tool @Whistleblowing.

The report must contain a detailed description of the facts and the conduct considered in breach of the regulations, also indicating, where possible, the documents, the rules that are considered to have been breached and other items useful for making a determination of the disputed facts. In addition, the reporting person is required to state whether he has a personal interest in making the report.

The @Whistleblowing tool ensures that it is impossible to hide or eliminate a report that has been sent.

The Head of the internal system for reporting breaches, the corporate body with a control function and the Supervisory Body are jointly involved in guaranteeing:

- retention of the documentation regarding the reports and the relative checks as well as the provisions on any decisions taken by the competent functions in appropriate hard copy/ICT files, ensuring suitable levels of security/confidentiality;
- storage of the documentation and the reports for a period of time not exceeding that required for the purposes for which originally collected and subsequently processed, and in any case in compliance with applicable personal data protection laws and regulations[13].

The Bank reserves the right to inflict specific penalties on the reporting person, where possible, if the related reports are made with wilful misconduct or gross negligence or if they should turn out to be false, unfounded, with defamatory content or in any case carried out with the sole purpose of harming the Bank, the reported person or other parties affected by the report. The Bank may additionally take the appropriate initiatives in a court of law. Excluding cases of responsibility for libel and defamation, or for the same pursuant to article 2043 of the Italian Civil Code, the existence of a report as part of the procedure referred to in paragraph 1 does not constitute a breach of the obligations deriving from an employment relationship[14].

The report is acquired by the Head of the internal system for reporting breaches, who immediately initiates an analysis procedure, also using the collaboration of other departments within the Bank or external resources (e.g. consultants, forensic analysts, technicians, private investigators). All investigations must be conducted on a timely basis, without continuing for longer than is reasonably necessary given the subject of the report[15]. The investigation must be conducted with impartiality and independence. No person with a conflict of interest

[13] Legislative Decree no. 196 of 30 June 2003, as amended by Legislative Decree no. 101 of 10 August 2018; Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 (articles 5, 15 and 23).
[14] Article 4-undecies of the TUF.
[15] Regulation on provisions implementing Legislative Decree no. 58 of 24 February 1998 on market matters (article 60-bis) (adopted by Consob by way of Resolution no. 20249 of 28 December 2017).

may be involved in the enquiries or decision-making process, nor anyone who might be responsible for the failure to adopt measures designed to prevent or detect the alleged breaches. Current or potential conflicts of interest must be promptly reported by any persons involved in the investigations to the Head of Whistleblowing or to the Chairman of the Management Control Committee if the Head of Whistleblowing finds himself in a situation of conflict of interest. The outcome of the investigation will be communicated to the reporting person within a period not exceeding three months from the acknowledgment of receipt.

The investigations are performed with the utmost confidentiality at all levels, from the receipt of the report to the completion of the procedure. Confidentiality applies to the facts under investigation, to the person(s) involved, to the subject of the report, to the procedure being followed, to the materials and information gathered and to the results of the procedure. The persons involved in the investigations must not disseminate information to anyone not directly involved in such investigations.

The procedure adopted by the company ensures the confidentiality of the personal data of the reporting person and the person allegedly responsible for the breach, in accordance with the requirements of privacy laws and regulations, without prejudice to the rules governing any investigations or proceedings initiated by the judicial authorities in respect of the facts contained in the reporting. The parties receiving, examining and assessing the reports, the Head of the internal system for reporting breaches and any other person involved in the process are required to ensure the confidentiality of the information received, also with respect to the identity of the reporting person who, in any case, must be suitably protected from retaliatory, discriminatory or in any case unfair conduct as a result of the reporting.

If, subsequent to further detailed analysis, the report turns out to be unfounded, it will be filed and no further action of any kind will be taken[16]. On the other hand, if a breach is discovered, the Head of the internal system for reporting breaches immediately informs the corporate body with a control function, the corporate body responsible for strategic supervision, the Supervisory Body and any organisational unit involved about this, as well as informing the reporting person and possibly also the reported parties, also for the purpose of identifying and deciding on the most appropriate measures to be taken, in accordance with the requirements of the company's disciplinary system in force at the time, and to inform the authorities if there is a legal requirement in that sense. In either case, at the end of the procedure the reporting person is informed that the procedure has been concluded[17].

The above-mentioned systems are structured in such a way as to ensure that reports are received, examined and assessed by way of specific, autonomous and independent channels that are separate from ordinary lines of reporting. To this end, due to the way they are configured (ICT channel and ordinary channel with letter box), the internal reporting systems ensure the availability of an alternative channel for the reporting person, guaranteeing that the person in charge of receiving, examining and assessing the report is not hierarchically or functionally subordinate to any reported person, is not the person allegedly responsible for the breach and does not have a potential interest linked to the reporting that may compromise the impartiality and independence of his judgement. If the reporting person is jointly responsible for the breaches, it would be better if he were to receive privileged treatment compared to the other jointly responsible persons, compatible with the applicable discipline[18].

In any event, Circular no. 285 of the Bank of Italy of 17 December 2013 requires that the persons responsible for receiving, examining and assessing the reports should not participate in the adoption of any decision-making provisions, which are remitted to the competent corporate functions or bodies.

6.1 The Supervisory Body

The Supervisory Body has a complete view of any reporting through the @Whistleblowing tool and can decide whether to initiate an assessment procedure or dismiss the case, documenting the reasons for the decision in the minutes of the meeting at which the report is discussed.
If the Supervisory Body decides to carry out an assessment or go into further detail, it minutes whether the assessment activities will be performed with the support of certain specific business functions or instead by using the services of external resources (for example consultants, forensic analysts, technicians, private investigators).
On completion of the assessment or after going into further detail, and on the basis of the results of such work,

[16] ABI 2015 Guidelines: point 8.
[17] ABI 2015 Guidelines: points 7 and 9.
[18] Circular no. 285 of 17 December 2013, "Supervisory provisions for banks", Part I, Title IV, Chapter 3, Section VIII.

the Supervisory Body:

a. dismisses the case if the reporting turns out to be unfounded;
b. calls for further work to be done;
c. provides the functions concerned with its recommendations;
d. assesses, together with the competent business functions, the need for any disciplinary measures to be taken against the persons involved and any steps required to protect the Group's interests.

7 MEASURES TO PROTECT THE PERSONS INVOLVED

7.1 Confidentiality of the personal data of the reporting person

The Bank puts suitable controls in place to ensure the confidentiality of the personal data of the reporting person and of the person allegedly responsible for the breach.

The information and any other item of personal data acquired in applying these rules are processed in full compliance with Legislative Decree no. 196 of 30 June 2003, Regulation (EU) 2016/679 on the protection of natural persons with regard to the processing of personal data and any subsequent measures on the subject ("Privacy Legislation").

More specifically, pursuant to and in accordance with article 11 of Legislative Decree no. 196/2003, personal data processed for the purpose of these rules must be:

- restricted to data strictly and objectively necessary for checking the validity of the reporting and for managing this;
- processed lawfully and properly.

The @Whistleblowing platform, which is available to all reporting persons, contains information on the protection of the personal data processed in application of these rules.

7.2 Protecting the reporting person from retaliatory action

Pursuant to article 52-bis of the TUB and pursuant to article 6, paragraph 2-bis of Legislative Decree no. 231/2001, the Bank provides appropriate protection for the reporting person "against retaliatory, discriminatory and in any case unfair conduct as a result of the reporting", in a climate of respecting the dignity of such.

illimity Bank safeguards reporting persons against any form of retaliation, discrimination and penalisation and in all cases ensures full and complete confidentiality of their identity, excluding any legal obligations. Pursuant to article 6 of Legislative Decree no. 231/2001:

- direct or indirect retaliatory or discriminatory action taken against the reporting person for reasons connected directly or indirectly with the reporting is forbidden. Retaliatory dismissal and organisational measures having direct or indirect negative effects on working conditions are null and void, unless it can be shown that they are not of a retaliatory nature and are based on reasons not connected with the reporting;
- any adoption of discriminatory measures can be reported to the national labour inspectorate;
- the internal disciplinary system envisaged by Legislative Decree no. 231/2001 is applicable to employees who:
  - breach confidentiality rules on the identity of the reporting person or the prohibition of discriminatory or retaliatory action;
  - report facts that turn out to be unfounded by way of wilful misconduct or gross negligence.

8 ANNEXES

8.1 ANNEX 1: RELATED LEGISLATION AND REGULATIONS

INTERNAL RELATED REGULATIONS

Organisation, Management and Control Model
illimity Way

EXTERNAL RELATED LEGISLATION AND REGULATIONS

Legislative Decree no. 231 of 8 June 2001
Circular no. 285/2013 of the Bank of Italy