de volksbank

De Volksbank N.V. Information Statement with the Purpose to Facilitate Due Diligence Undertaken by Our Foreign Correspondent Relations

September 2019

To Whom It May Concern:

De Volksbank N.V. (further referred to as "the Bank") is pleased to send you this Information Statement.

In line with regulatory obligations and international best practices related to anti-money laundering (AML) and customer due diligence (CDD) measures for correspondent relationships[1], financial institutions gather information about their foreign respondents 'and other counterparties' business and their AML/CDD controls. The Bank has correspondent and other relationships with several foreign financial institutions, and as a result, regularly receives CDD inquiries from its foreign correspondent partners and other counterparties.

The purpose of this Information Statement is to facilitate CDD undertaken by our foreign correspondent relationships and counterparties, and to provide them with important information concerning:

- I. Description of the Bank, Ownership, Nature of the Bank's Business and the Market it Serves;
- II. AML and Supervisory Regime of the Jurisdiction that Issued the License to the Bank;
- III. CDD/AML and Sanctions Policies and Procedures of the Bank;
- IV. Certification Regarding Correspondent Accounts for Foreign Banks;
- V. Type, Purpose and Anticipated Activity of Foreign Correspondent Accounts;
- VI. Correspondent Banking Services to Foreign Financial Institutions.

The information contained herein complements the information provided by the information contained in the Bank's Wolfsberg Group AML Questionnaire, and the Bank's "Certification regarding Correspondent Accounts for Foreign Banks" pursuant to Sections 5318(j) and 5318(k) of Title 31 of the United States Code as added by sections 313 and 319(b) of the USA Patriot Act of 2001 (Public Law 107-

[1] EU Directive on Money Laundering, 2014 Wolfsberg Anti-Money Laundering Principles for Correspondent Banking, and national legislation such as Sections 5318(j) and 5318(k) of Title 31 of the United States Code, and U.K Money Laundering Regulations 2007, No. 2157, Part 2, Regulation 14.

56) and both available on our Bank's website[2] and the SWIFT KYC Registry system.

1 Description of the Bank, Ownership, Nature of the Bank's Business and the Market it Serves

Overview and ownership

De Volksbank N.V. is a bank with a banking license from the Netherlands. With its activities de Volksbank N.V. offers a balanced range of brands like SNS, ASN Bank, RegioBank and BLG Wonen.

The Bank has a balance sheet total of € 61 billion[3] and approximately 3,797 employees (FTEs)[4], making it a relevant player in the Dutch market. The bank has its headquarters in Utrecht, the Netherlands.

With effect from March 30th 2019 Stichting administratiekantoor beheer financiële instellingen (NL Financial Investments, 'NLFI'[5]) is the sole shareholder of de Volksbank N.V.

Organization, products, services and clients

The Bank approaches its market, the Netherlands, with several brands:

- **SNS** is the general consumer brand for people looking to manage their financial affairs with an accessible service. SNS wants to compete in the banking market for consumers and self-employed persons, with distinguishing customer propositions that break through existing conventions. The core products are payments, savings, mortgages and insurance.
- **ASN Bank** is the brand for sustainable savings, investments and payments. ASN Bank focuses primarily on retail customers, but also counts social organizations and companies among its customers that wish to manage or invest their money in a responsible manner.
- **RegioBank** is the brand for people who consider a local and personal service and a link with the local community to be important.

---

[2] www.devolksbank.nl/en

[3] financial report 2018 de Volksbank, P. 5.

[4] financial report 2018 de Volksbank, P. 5.

[5] NFLI is the sole shareholder of de Volksbank N.V. The shares in de Volksbank N.V. were transferred to NFLI by the Dutch State.
The establishment of NLFI was the result of a parliamentary resolution to ensure a commercial, non-political governance of financial institutions, and a transparent separation of interests. See: http://www.nlfi.nl/what-we-do.

- **BLG Wonen** is the brand for people who prefer to take a wide range of advice on financing their home from their independent adviser.

This Statement covers the above-mentioned entity and brands.

In general, the Bank does *not* intend to engage in activities such as:

- trade finance;
- offshore banking;
- downstream clearing services;
- nested accounts.

2 AML and Supervisory Regime of the Jurisdiction that Issued the License to the Bank

Jurisdiction

The Bank is located and maintains a physical presence in the Netherlands, Europe, where the Bank is authorized to conduct banking activities. The physical street address is Croeselaan 1, 3521 BJ, Utrecht, where the Bank maintains employees and operational records related to its banking activities.

The Bank does not have a major presence outside the Netherlands.[6] The Bank currently does not have any presence, nor has any future plans to have presence, in any of the currently sanctioned countries such as Burma/Myanmar, Cuba, Iran, North Korea, Republic of Sudan, Syria or Zimbabwe.

License

The Bank has a banking license[7] issued by De Nederlandsche Bank (DNB), one of the supervisors for banks and other financial institutions.

The brands of the Bank: SNS, ASN Bank, RegioBank and BLG Wonen are covered by the license of the Bank.

Furthermore, the Bank is *not* operating under any of the following:

- an offshore license;[8]

[6] Please note that the Bank has a EU Passport for the UK for purposes of participation in a bonds program, see http://www.dnb.nl/toezichtprofessioneel/de-consument-en-toezicht/registers/WFTKF/detail.jsp?id=94bbcae35848e311b55a005056b672cf, and the Bank, has a 25% participation in investment firm TripleJump B.V., headquartered in Amsterdam, the Netherlands, with locations in Bangkok, Lima, Mexico City, Tbilisi and Nairobi.

[7] License can be found at: http://www.dnb.nl/toezichtprofessioneel/de-consument-en-toezicht/registers/WFTKF/detail.jsp?id=94bbcae35848e311b55a005056b672cf.

[8] The USA PATRIOT Act (31 USC 5318(i)(4)(A) and 31 CFR 1010.605(i) define an offshore banking license as a license to conduct banking activities that, as a condition of the license,

- a banking license issued by a foreign country that has been designated as non-cooperative with international AML principles or procedures by the Financial Action Task Force (FATF);
- a banking license issued by a foreign country that has been designated by the U.S. Secretary of the Treasury as warranting special measures due to money laundering concerns.

For this reason, the enhanced due diligence controls required by 31 CFR 1010.610(b) for our U.S. correspondent relations are not applicable to the Bank.

Supervisory regime

DNB supervises the Bank for its compliance with the "Wet ter Voorkoming van Witwassen en Financiering van Terrorisme" (WWFT)[9] and the "Sanctiewet 1977" [10] (further described below under section "AML and sanctions regime of the Netherlands").

In addition, the Bank is supervised by the European Central Bank.

AML and sanctions regime of the Netherlands

It may be appropriate for an institution to consider the fact that the Bank operates in and is subjected to a regulatory environment that is internationally recognized as adequate in the fight against money laundering: The Netherlands, Europe.

The Netherlands is located in the top 10 of countries with the *lowest* Corruption Perceptions Index of Transparency International.[11]

The Netherlands is a member of the Financial Action Task Force (FATF) and subscribes to its recommendations on measures to combat money laundering and terrorist financing.

In accordance with the FATF recommendations and the EU Anti-Money Laundering Directive, the Netherlands has enacted laws and created legislative and regulatory standards to deter money laundering, terrorist financing, and other illicit activities, in particular the WWFT, and Sanctiewet 1977.

Money laundering is a criminal offense in the Netherlands, and financial institutions are required to establish internal policies, procedures, and systems for the detection and prevention of money laundering throughout their worldwide operations.

---

prohibits the licensed entity from conducting banking activities with the citizens, or in the local currency of, the jurisdiction that issued the license.

[9] Prevention of Money Laundering and the Financing of Terrorism Act of 2008.

[10] Sanction Law of 1977.

[11] https://www.transparency.org/cpi2018

The Bank has policies and procedures to comply with these laws and regulations that are monitored by regulatory entities responsible for AML/CDD compliance. These policies are further described in section III of this Statement.

The main customer identification, CDD and continuous monitoring requirements under the WWFT are set out below.

Art 3 (1) of the WWFT lists the following actions the institution needs to take when conducting CDD:

a) establish and verify the identity of the *customer*;
b) identify the customer's *ultimate beneficial owner*[12] and implement adequate risk-based measures to verify the ultimate beneficial owner's identity and, when the client is a legal person, to implement adequate risk-based measures to understand the customer's ownership and control structure;
c) establish the objective and intended nature of the business relationship;
d) conduct continuous monitoring of the business relationship and the transactions carried out during the existence of this relationship to ensure that these are consistent with the knowledge the institution has of the customer and the customer's risk profile and, where relevant, examine the source of the assets used for the business relationship or the transaction;
e) establish that the natural person who represents the customer is authorized to do so;
f) implement adequate risk-based measures to verify whether the customer is acting on his/her own behalf or for a third party;
g) as the occasion arises, establish and verify the identity of the natural person referred to in (e).

The WWFT also requires the Bank:

- to conduct enhanced due diligence on Politically Exposed Persons;
- to report, without delay, unusual transactions based on objective and subjective indicators to the Dutch Financial Intelligence Unit (FIU);[13]

[12] Art.1(f) of the WWFT defines the *ultimate beneficial owner* as: the natural person who: 1° holds a share of more than 25% in the issued capital of a customer; 2° can exercise more than 25% of the voting rights at the general meeting of shareholders of a client; 3 ° can exercise actual control over a customer; 4 °is the beneficiary of 25% or more of the assets of a customer or trust; or 5° has special control over 25% or more of the assets of a customer, unless the customer is a company subjected to disclosure requirements as referred to in EU Directive 2004/109/EC (publicly listed companies).

[13] In accordance with the WWFT, covered institutions have a legal duty to report unusual transactions to the Financial Intelligence Unit (FIU-Netherlands). See: http://en.fiu-nederland.nl. The FIU-Netherlands is the equivalent agency of Financial Crimes Enforcement Network of the U.S. and the National Crime Agency in the United Kingdom. FIU-Netherlands is a member of the Egmont Group of Financial Intelligence Units. See: http://www.egmontgroup.org/about/list-of-members/by-region/europe.

- to train staff on requirements of the WWFT, including CDD and ongoing monitoring requirements, insofar as relevant for the execution of their tasks, and to ensure that staff are trained on a regular basis to be able to recognize unusual transactions and conduct CDD.

Furthermore, Dutch financial institutions, including our Bank, are under obligation for compliance with European Union and other international sanctions regulations, with regard to for example Burma/Myanmar, Iran, North Korea, Republic of Sudan, Syria and Zimbabwe.

The Sanctiewet 1977 is the basis for the implementation in the Netherlands of (inter)national rules regarding international sanctions. This framework law offers the possibility to impose general administrative measures with respect to compliance with treaties or international sanctions agreements.

3 CDD/AML and Sanctions Policies and Procedures of the Bank

Written policies, procedures, and compliance framework

Policy on client integrity
The Bank maintains written policies and procedures regarding client integrity[14], with detailed risk-based AML/CFT[15] policies and procedures, covering the requirements of the Dutch laws and regulations on AML/CFT.

The policy regarding client integrity is applicable to the Bank and its brands and employees, updated regularly and is approved by the Non-Financial Risk Committee of de the bank.

This policy includes a strong corporate policy statement that the Bank will:
- take all reasonable measures to only accept clients with a good reputation;
- take all reasonable measures to detect instances of money laundering or terrorist financing;
- take all reasonable measures to cooperate with the applicable authorities in their work to implement anti-money laundering and counter terrorist financing laws, and;
- work with the supervisory agencies in maintaining this policy and implementing measures to achieve these goals.

This policy covers:
- detailed customer due diligence and customer acceptance, including verification of beneficial owner(s) in line with the WWFT;
- risk classification of customers, including procedures to articulate what constitutes a high risk customer (e.g. Politically Exposed Persons and commercial real estate customers);

[14] This document is called "Beleid Klant Acceptatie, Monitoring en Review de Volksbank N.V." (Policy Client acceptance, monitoring and review).
[15] CFT: Counter Terrorist Financing

- ongoing monitoring (Event Driven Review and Periodic Driven Review);
- AML-monitoring transactions;
- client and transaction filtering against sanction and terrorism lists;
- reporting of unusual transactions;
- Record retention;
- Training.

Sanctions regulation policy

First of all, it should be noted that the Bank's sanctions risk is low, due to the fact that the vast majority of the Bank's business is domestic retail transactions, the Bank has negligible presence abroad[16], and does not have any presence or operations in any of the sanctioned countries. The Bank does not engage in any transactions or payments to or from Iran.

Additionally, the Bank maintains a detailed written policy[17] and procedures regarding compliance with (inter)national sanctions laws and regulations, and U.S. sanctions laws and regulations, where applicable.[18]

The Bank maintains a stricter policy than sanction regulations requires on certain high sanction risk countries. The Bank does not engage in any transactions or payments to or from these counties. The stricter policy is written in a Statement (in Dutch), which is published on the corporate website of the Bank[19].

The Sanctions regulations Policy is applicable to the Bank and its brands and employees, updated regularly and is approved by the Non-Financial Risk Committee of the bank

Compliance director

The Bank has a Compliance Director who reports directly to the Chief Risk Officer, and the Supervisory Board of the Bank.

CDD/AML and Sanctions training

The CDD/AML and Sanctions Policies of the Bank dictates that employees are familiar with the contents of the WWFT and AML/Sanctions Policies of the Bank. The Bank has set up a Training & Awareness Programme, in which the themes related to CDD/AML and Sanctions are structurally guaranteed.

---

[16] See section II of this Information Statement, under heading "jurisdiction".

[17] This document is called "Beleid naleving sanctieregelgeving de Volksbank N.V."(Sanction regulations policy).

[18] For example: It is the policy of the Bank to check clients and beneficiaries in non-domestic transactions against the OFAC list and the FinCEN Section 311 List.

[19] https://www.devolksbank.nl/assets/files/Statement-naleving-sanctieregelgeving-de-Volksbank.pdf

All employees are classified into educational levels. The Bank provides a mandatory e-learning module on an annual basis to all employees. In addition, the Bank provides periodic classroom training/workshops on different themes in the field of CDD/AML and Sanctions (with both internal and external trainers) and several mandatory and customized e-learning modules to relevant employees, including:

- Employees who have contacts with customers;
- Employees who process and analyze customers and transactions;
- Employees with client relationship tasks;
- Employees working for the Compliance department.

The CDD/AML and Sanctions Policies further provide for annual CDD/AML and Sanctions training for the board and senior management.

Independent review/auditing

The Bank has arrangements for the independent auditing and review of compliance with the WWFT and Sanctiewet 1977 policies and procedures. This is done by both internal audit, and a "big four" public accounting firm on an annual basis.

Monitoring and reporting of unusual transactions

The Bank currently uses commercial transaction monitoring software, including Norkom, RiskShield and Dow Jones to monitor transactions. The Bank's Security Department investigates AML, sanctions alerts and fraud incidents. In case of an unusual transaction the Bank will report this transaction to the FIU.

In cases of a sanction "hit" as defined in the Regeling Toezicht Sanctiewet 1977 the Bank will:

- report this "hit" to DNB or the AFM and if applicable to the FIU;
- reject the transaction and/or freeze the assets (whatever is applicable).

Record keeping

The Bank maintains records related to Customer Due Diligence in the customer files for a period of five years after termination of the service or termination of the relationship. Records regarding reports of unusual transactions sent to the Financial Intelligence Unit are also kept for a period of five years.

4 Certification Regarding Correspondent Accounts for Foreign Banks

Our Bank maintains a "Form of Certification Regarding Correspondent Accounts – Certification Regarding Correspondent Accounts for Foreign Banks" pursuant to

Section 5318(j) and 5318(k) of Title 31 of the United States Code, added by Sections 313 and 319(b) of the USA Patriot Act of 2001 (Public Law 107-56). This can be obtained at our Bank's website and SWIFT KYC Registry, mentioned on page 1 of this Information Statement.

CT Corporation System[20] is authorized to accept services of legal process on behalf of our Bank pursuant to Section 5318(k) of Title 31, United States Code.

5 Type, Purpose and Anticipated Activity of Foreign Correspondent Accounts

The Bank maintains correspondent relationships with foreign financial institutions to enable us to provide customers with cross-border products and services that we cannot provide ourselves, typically because the Bank lacks an international network.

The below chart shows, which types of transactions the Bank, in general, intends to process through its correspondent accounts at foreign financial institutions:

Cash clearing	YES
Liquidity management	YES
(Short term) Borrowing	YES
For its own investment needs in a particular currency	YES
Cash management (e.g. interest bearing accounts in foreign currency)	YES
Check clearing	NO
Execution of third party payments (for customers of the Bank)	YES
Foreign exchange services	YES
Trade finance	NO
Pouch activity	NO
Use as Payable Through Account	NO
Credit card transactions	YES
Securities transactions	YES

6 Correspondent Banking Services to Foreign Financial Institutions

The Bank does not offer correspondent banking services to other financial institutions, with the following limited exceptions:

1. Cecabank S.A. in Spain[21]

[20] CT Corporation System is a resident of the United States at the following street address: 111 8th Avenue, New York, NY 10011.
[21] http://www.cecabank.es/en/quienes-somos/sobre-nosotros/.

Cecabank maintains a regular online corporate banking account with our Bank, which is used as a "collection account" for pension agreement operations and other Euro transactions for Cecabank clients. The collected amount of money is after a certain period transferred by the Bank to Cecabank's Loro account at our Bank and after that, transferred by our Bank to Cecabank so they can transfer the money into the accounts of their clients.

The transactions offered to Cecabank are payment transactions in Euros, and do not involve foreign currency, such as U.S. dollars or pounds Sterling. This means that these transactions for Cecabank customers will **not** be processed through our Bank's U.S. or U.K. correspondent accounts. Therefore, it is unlikely that Cecabank, our Spanish respondent will "nest" in a U.S. or U.K. correspondent account the Bank maintains.

2. The Bank has exchanged SWIFT keys[22] with a number of other financial institutions.

For these relationships, in practice, the Bank

- does not function as "intermediary correspondent", and thus only conducts financial transactions for the SWIFT key holding entities, whereby one of the parties (either originating or beneficiary) in the transaction is the Bank's own client;
- only conducts payment transactions or other messages, such as queries, answers and free format messages for our own customers;
- does not conduct trade finance transactions;
- does not process checks or money orders.

The AML Policy of the Bank dedicates a section to risk management related to correspondent relationships, and dictates that correspondent relations with banks in non-EER countries are subject to enhanced due diligence, which includes investigating the procedures of the respondent, and covers issues such as:

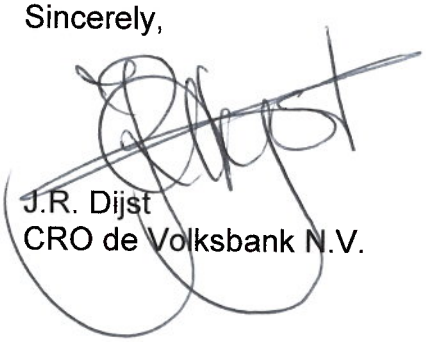
- nature of activities of the respondent;
- procedures related to the prevention of money laundering and terrorist financing;
- to what extent has the correspondent identified its clients, and verified the identity, and conducts ongoing customer due diligence;
- what is the nature of the correspondent relationship;
- that the Bank can ensure that the respondent can provide appropriate client information at the Bank's request.

[22] We are including the SWIFT key exchanges in this Information Statement, due to the fact they are sometimes considers an equivalent of a traditional correspondent relationship. See for example the Wolfsberg Principles 2014 on correspondent banking, Section 2, indicating that "These Principles may also be applied to SWIFT Relationship Management Application (RMA) relationships in part, or in totality, using a risk-based approach".

Finally, according to the AML/CFT Policy of the Bank, and pursuant to the WWFT, it is prohibited to have correspondent relationships with shell banks or sanctioned financial institutions.

We are confident that this Information Statement will facilitate the due diligence conducted on the Bank, and remain at your disposal for additional information you may need.

Sincerely,



J.R. Dijst
CRO de Volksbank N.V.