

Vyhlásenie banky k ochrane pred legalizáciou príjmov z trestnej činnosti a financovaním terorizmu

Poštová banka, a.s., jej štatutármi zástupcovia, vedúci aj radoví zamestnanci si uvedomujú závažnosť a spoločenskú nebezpečnosť legalizácie príjmov z trestnej činnosti a financovania terorizmu (ďalej len „legalizácia“), ako aj aktuálnosť a naliehavosť plnenia úloh stanovených slovenskou legislatívou, českou legislatívou, banka vychádza aj z európskej legislatívy, z odporúčaní Bazilejského výboru pre bankový dohľad a Wolsbergských zásad, z odporúčaní FATF a v záujme ich zabezpečenia má banka spracovanú koncepciu ochrany pred legalizáciou a program činnosti zameranej proti legalizácii spracovaný v zmysle zákona, ktorého významnú súčasť tvoria najmä:

- základné faktory pre hodnotenie rizikovosti klientov, obchodných vzťahov, druhov obchodov, ako aj rizikové faktory jednotlivých obchodných operácií, ktoré sú premietnuté do prehľadu foriem neobvyklých obchodných operácií,
- požiadavky na vykonanie starostlivosti o klienta v závislosti od rizika legalizácie,
- metodiku postupu pri predchádzaní legalizácie a pri jej odhaľovaní, ktorej základom je spoľahlivé vykonávanie a overovanie identifikácie zákonom predpísaným spôsobom za fyzickej prítomnosti klienta, postupy pre posudzovanie obvyklosti obchodných operácií a monitorovanie klientov a ich obchodných operácií,
- postupy na odmietnutie, zdržanie a ohlásenie neobvyklej obchodnej operácie, ak by jej vykonaním mohlo dôjsť k legalizácii,
- obsah a harmonogram odbornej prípravy zamestnancov.

Banka v súvislosti s vykonávaním základnej starostlivosti vo vzťahu ku klientom

- neuzavrie obchodný vzťah a neuskutoční obchod s anonymným klientom alebo s tzv. „shell bankou“,
- zisťuje, či klient nie je politicky exponovanou osobou alebo osobou, na ktorú boli vyhlásené medzinárodné sankcie,
- pri právnických osobách - podnikateľoch a združeniach majetku môže v závislosti od rizika legalizácie požadovať identifikáciu konečných užívateľov výhod, zisťovať vlastnícku štruktúru a riadiacu štruktúru klienta a žiadať aj overenie identifikácie za fyzickej prítomnosti v banke alebo iným zákonom určeným spôsobom,
- zisťuje informácie o účele a plánovanej povahe obchodného vzťahu, vykonáva monitorovanie obchodného vzťahu a obchodných operácií, zisťuje pôvod finančných prostriedkov použitých v obchodnej operácii a vyžaduje na tento účel relevantné doklady a informácie o klientoch.

Vyššie uvedené opatrenia sú zamerané predovšetkým na prevenciu pred legalizáciou ako aj na ochranu klienta banky. Banka k nim pristupuje s plnou vážnosťou a vykonáva ich z dôvodu svojej ochrany pred zneužitím na pranie špinavých peňazí a celospoločensky naliehavej požiadavky ochrany pred terorizmom, z toho dôvodu sa členovia štatutárneho orgánu zaviazali na dodržiavanie týchto zásad v zmysle Stanov Poštovej banky, a.s. a spolu so zamestnancami banky v zmysle Organizačného poriadku Poštovej banky, a.s. a Kompetenčného poriadku Poštovej banky, a.s.

Dôsledná identifikácia a overovanie identifikácie klientov a požadovanie súvisiacich dokladov a ďalších informácií môže vo Vás vyvolávať pocit prílišného administratívneho zaťaženia, chceme ju však chápať ako našu spoločnú daň v záujme bezpečnosti každého z nás a zároveň aj ako ochranu pred zneužitím Vašich prostriedkov osobami využívajúcimi nelegálne a podvodné praktiky.

Predstavenstvo Poštovej banky, a.s.

Financial Institution Name: Poštová banka, a.s.

Location: Dvořákovo nábrežie 4, 811 02 Bratislava, Slovak Republic

This questionnaire acts as an aid to firms conducting due diligence and should not be relied on exclusively or excessively. Firms may use this questionnaire alongside their own policies and procedures in order to provide a basis for conducting client due diligence in a manner consistent with the risk profile presented by the client. The responsibility for ensuring adequate due diligence, which may include independent verification or follow up of the answers and documents provided, remains the responsibility of the firm using this questionnaire.

Anti-Money Laundering Questionnaire

If you answer "no" to any question, additional information can be supplied at the end of the questionnaire.

I. General AML Policies, Practices and Procedures:	Yes	No
1. Is the AML compliance program approved by the FI's board or a senior committee?	Yes	-
2. Does the FI have a legal and regulatory compliance program that includes a designated officer that is responsible for coordinating and overseeing the AML framework?	Yes	-
3. Has the FI developed written policies documenting the processes that they have in place to prevent, detect and report suspicious transactions?	Yes	-
4. In addition to inspections by the government supervisors/regulators, does the FI client have an internal audit function or other independent third party that assesses AML policies and practices on a regular basis?	Yes	-
5. Does the FI have a policy prohibiting accounts/relationships with shell banks? <i>(A shell bank is defined as a bank incorporated in a jurisdiction in which it has no physical presence and which is unaffiliated with a regulated financial group.)</i>	Yes	-
6. Does the FI have policies to reasonably ensure that they will not conduct transactions with or on behalf of shell banks through any of its accounts or products?	Yes	-
7. Does the FI have policies covering relationships with Politically Exposed Persons (PEP's), their family and close associates?	Yes	-
8. Does the FI have record retention procedures that comply with applicable law?	Yes	-
9. Are the FI's AML policies and practices being applied to all branches and subsidiaries of the FI both in the home country and in locations outside of that jurisdiction?	Yes	-

The Wolfsberg Group consists of the following leading international financial institutions: Banco Santander, Bank of Tokyo-Mitsubishi UFJ, Barclays, Citigroup, Credit Suisse, Deutsche Bank, Goldman Sachs, HSBC, JP Morgan Chase, Société Générale and UBS which aim to develop financial services industry standards, and related products, for Know Your Customer, Anti-Money Laundering and Counter Terrorist Financing policies.

II. Risk Assessment:		Yes	No
10. Does the FI have a risk-based assessment of its customer base and their transactions?		Yes	-
11. Does the FI determine the appropriate level of enhanced due diligence necessary for those categories of customers and transactions that the FI has reason to believe pose a heightened risk of illicit activities at or through the FI?		Yes	-
III. Know Your Customer, Due Diligence and Enhanced Due Diligence:		Yes	No
12. Has the FI implemented processes for the identification of those customers on whose behalf it maintains or operates accounts or conducts transactions?		Yes	-
13. Does the FI have a requirement to collect information regarding its customers' business activities?		Yes	-
14. Does the FI assess its FI customers' AML policies or practices?		Yes	-
15. Does the FI have a process to review and, where appropriate, update customer information relating to high risk client information?		Yes	-
16. Does the FI have procedures to establish a record for each new customer noting their respective identification documents and 'Know Your Customer' information?		Yes	-
17. Does the FI complete a risk-based assessment to understand the normal and expected transactions of its customers?		Yes	-
IV. Reportable Transactions and Prevention and Detection of Transactions with Illegally Obtained Funds:		Yes	No
18. Does the FI have policies or practices for the identification and reporting of transactions that are required to be reported to the authorities?		Yes	-
19. Where cash transaction reporting is mandatory, does the FI have procedures to identify transactions structured to avoid such obligations?		Yes	-
20. Does the FI screen customers and transactions against lists of persons, entities or countries issued by government/competent authorities?		Yes	-
21. Does the FI have policies to reasonably ensure that it only operates with correspondent banks that possess licenses to operate in their countries of origin?		Yes	-
22. Does the FI adhere to the Wolfsberg Transparency Principles and the appropriate usage of the SWIFT MT 202/202COV and MT 205/205COV message formats? ¹		Yes	-
V. Transaction Monitoring:		Yes	No
23. Does the FI have a monitoring program for unusual and potentially suspicious activity that covers funds transfers and monetary instruments such as travelers checks, money orders, etc?		Yes	-

¹ The four payment message standards to be observed are: i) FIs should not omit, delete, or alter information in payment messages or orders for the purpose of avoiding detection of that information by any other FI in the payment process; ii) FIs should not use any particular payment message for the purpose of avoiding detection of information by any other FI in the payment process; iii) Subject to applicable laws, FIs should cooperate as fully as practicable with other FIs in the payment process when requesting to provide information about the parties involved; and (iv) FIs should strongly encourage their correspondent banks to observe these principles. Source: [http://www.wolfsberg-principles.com/pdf/standards/Wolfsberg_NYCH_Statement_on_Payment_Message_Standards_\(2007\).pdf](http://www.wolfsberg-principles.com/pdf/standards/Wolfsberg_NYCH_Statement_on_Payment_Message_Standards_(2007).pdf)

The Wolfsberg Group consists of the following leading international financial institutions: Banco Santander, Bank of Tokyo-Mitsubishi UFJ, Barclays, Citigroup, Credit Suisse, Deutsche Bank, Goldman Sachs, HSBC, JP Morgan Chase, Société Générale and UBS which aim to develop financial services industry standards, and related products, for Know Your Customer, Anti-Money Laundering and Counter Terrorist Financing policies.

