RESEARCH PAPERS OF WROCŁAW UNIVERSITY OF ECONOMICS
No. 85 — 2009
Advanced Information Technologies for Management – AITM 2009

Elżbieta Iwonin

Citi Handlowy, Warsaw, Poland
e-mail: elzbieta.iwonin@citi.com

IMPLEMENTATION OF AML DIRECTIVE INTO POLISH LEGAL SYSTEM – CITI HANDLOWY EXPERIENCE

Abstract: The purpose of the article is to clarify interesting aspects and the positive results of the consultation process during the legislative works on the project of amendment of the Act on Counteracting Introduction into Financial Circulation of Property Values derived from Illegal or Undisclosed Sources and on Counteracting the Financing of Terrorism of November 16, 2000 – Polish AML Act. The article is an attempt to predict the potential problems the covered institutions may have in the implementation process what was described in Section 4. The rest of the article presents new approach to the relationship with the customer imposed by the Directive and the impact which new obligations may have on covered institutions. There are proposals how the internal procedures need to be amended, how the customers should be verified and finally what minimal enhancements of the systems supporting the process are required. Citi Handlowy, being the subsidiary of the US financial institution, has already implemented many elements of new AML Act as a result of applying of FATF[1] regulations by the Parent Company. Based on this experience the article focuses on practical aspects of Know Your Customer programme implementation.

1. Active participation of banks' representation in the legislation process

1.1. The Directive 2005/60/EC on the prevention of the use of the financial system for the purpose of money laundering and terrorist financing was issued on 26 October 2005. According to the provision of paragraph 45, the Member States should adjust the national laws to the stipulations of the Directive by 15 December 2007. Changes to the "Act on Counteracting Introduction into Financial Circulation

[1] The Financial Action Task Force (FATF) is an inter-governmental body whose purpose is the development and promotion of national and international policies to combat money laundering and terrorist financing. The FATF is therefore a "policy-making body" created in 1989 that works to generate the necessary political will to bring about legislative and regulatory reforms in these areas. The FATF has published 40 + 9 Recommendations in order to meet this objective.

of Property Values derived from Illegal or Undisclosed Sources and on Counteracting the Financing of Terrorism" of November 16, 2000 (so-called "Polish AML Act") were required. There were three attempts to the implementation of the Directive in Poland – projects dated July 2007, 26 May 2008 and 19 December 2008.

1.2. First project of the implementation of the Directive into Polish AML Act was disclosed on FIU's[2] website in July 2007. It started a wide discussion in banking industry, which concentrated on the following problems.

a) The project was prepared only 5 months before the deadline imposed by the Directive, what significantly limited the time for the covered institutions to make them prepared. Initial proposal was 3 months for adjustment of internal procedures and 3 months for risk rating of existing customers.

b) Some provisions and definitions from the Directives have not been precisely and adequately copied into the Act. Among others the definition of the "beneficial owner", "shell bank", "business relationship" were not exactly the same as in the Directive.

c) The project maintained the obligation of registration and reporting the mass of transactions over 15,000 EUR. In 2006, 27 millions of transactions were subject to reporting by all covered institutions. The scope of information required in the Register of Transactions and the reports from the register was open. It was at the discretion of the Ministry of Finance how the final structure of information should be. For covered institutions, it meant the permanent readiness to adjust and enhance the system maintaining the Register of Transactions.

d) The project did not create the legal environment to give to the covered institutions the access to the government electronic database like PESEL, KRS imposing, at the same time, the duty to verify the customer's identity.

e) The project did not regulate the character of the relationship which covered institutions may have with the Politically Exposed Persons what was against the Directive.

f) The project did not assure the legal protection of the employees of the financial institutions adequate to this proposed by the Directive. The Directive protected all employees involved in the transaction reporting while the Project covered only those of the employees who were called to witness.

g) The project did not assure any legal protection for the financial institutions against claims resulted from the decision to refrain from carrying out suspicious transaction, when such decision has been taken in good faith. The banking industry proposed that it should be at the risk of the State Treasury.

h) The project imposed the enormous level of financial fine up to 3% of the annual revenue for the covered institution when it is not able to demonstrate the compliance with the Act.

---

[2] Financial Intelligence Unit. Polish abbreviation – GIIF. Government body dedicated for the supervision over money laundering and terrorism financing.

i) The project proposed very short period of time for the covered institutions to prepare the systems and procedures in accordance with new requirements.

j) Banking industry claimed the extended identification of the representatives of the customers being legal entities, while the Directive did not require such details of personal data. This aspect was a significant cost driver in the identification process in financial institutions and was the source of customers' dissatisfaction and frustration in the past.

1.3. Second project of the amendment of AML Act was published on 26 May 2008. At the end of June comments were made by the Polish Banks Association. Some of the issues raised by the banking industry were the same as previously; other came from new provisions proposed by the Ministry of Finance. The most important problems communicated to the regulatory were:

a) The delay in legislation process versus deadline 15 December 2007.

b) Some of the provisions were not interpreted in line with the Directive. The "beneficial owner" and "business relationship" are the examples.

c) Again the project maintained the obligation of registration and reporting the mass of transactions over 15,000 EUR. In 2007, 32 millions of transactions were subject to reporting by all covered institutions. The entire result of reporting efforts is unknown, FIU only reported the amount of blocked funds in 2007 – 7.1 million PLN, which does not seem to be adequate in comparison with the expenses spent in covered institutions to maintain the reporting system.

d) Moreover, the project extended the scope of information required in the Card of Transaction imposing the duty to register each transaction together with the information of the beneficial owner instead of recording the beneficial owner identity only once, during the due diligence.

e) Again, the project did not create the legal environment to give covered institutions the access to the government electronic database like PESEL, KRS in order to verify the identity of their customers. Without having a free of payment access to government databases, covered institutions have to rely on publicly known sources or commercial databases (further costs).

f) The project did not implement the art. 28 of the Directive – relaxation of banking secrecy in respect to disclosure information related to the prevention of money laundering and terrorist financing between institutions belonging to the same capital group.

g) Again, the project imposed too high level of financial fine up to 2% of the annual revenue of covered institution.

h) The order of implementation of particular provisions did not guarantee the effective investment in the information system; the deadline for publishing the executive acts was longer than the deadline for the adjustment of internal procedure in covered institutions.

i) Banking industry continued to criticise the scope of information required for the identification of the representatives of the customers being the legal entities. This

time banks asked to resign from collection of the address of the person arguing that PESEL and Identity Card number is sufficient to identify the person.

j) Consequently, the project did not assure legal protection for covered institutions against claims resulted from the decision to freeze the funds or refrain from processing the suspicious transaction, when such decision has been taken in good faith. The banking industry proposed that it should be at the risk of the State Treasury.

1.4. Final project dated 19 December 2008 was accepted by the Ministry of Finance on 6 January 2009. This version was sent to the Parliament. As the previous comments raised by Polish Bank Association were not addressed in the last project, they sent the list of outstanding issues directly to the Parliament – The Commission of the Public Financing. They repeated several concerns which related to:

a) significant delay in legislation process versus deadline 15 December 2007,

b) obligation of registering and reporting the mass of transactions over 15,000 EUR what is not required by the Directive and covered institutions should be released from this obligation,

c) lack of the legal environment to give to covered institutions the access to the government electronic database like PESEL, KRS in order to verify the identity of their customers,

d) lack of the protection for employees of covered institution from being exposed to threats or hostile action (art. 27 of the Directive),

e) lack of protection for covered institutions from being claimed by the customer as a result of the decision to freeze or refrain from processing of suspicious transaction, when such decision has been taken in good faith but was not confirmed by the decision of FIU,

f) unfavourable time schedule of implementation with regard to the particular provisions of the Act.

1.5. Polish Banks Association representatives have continued the consultation works in the Parliament Commission of the Public Financing. After the acceptance of the Parliament the revised AML Act was sent to the Senate in May 2009. At this stage the Polish Bank Association presented its last postulates related to unresolved areas as mentioned in items b)-e) above. The President countersigned the Act on 9 July 2009; it was published on 7 October 2009 and came into force in 14 days from publishing. Not all expectations of the banking industry have been met but some of areas were regulated successfully. The most positive changes are:

a) term deposits are excluded from the registration duty,

b) majority of definitions were corrected in accordance with the Directive provisions,

c) scope of information required in the identification process of the companies' representatives has been limited to the name and PESEL or the birthday date,

d) financial institutions have the right to inform the customer of actions taken by FIU against the account and this right cannot be revoked by the prosecutor,

e) 6 months for adjustment of internal procedures and 12 to perform due diligence of existing customers base,

f) the penalty level for the covered institutions limited to PLN 750,000,

g) exchange of information related to the money laundering aspects within covered institutions being the capital groups.

2. Most important changes imposed in the provisions of the Polish AML legislation forced by 3rd AML Directive

2.1. The list of changes which have been implemented into Polish AML Act is quite long but most of them related to the requirement of AML Directive. The key idea is the concept of Know Your Customer (KYC) called "due diligence". Due diligence tends to be Normal – as listed in art. 8b, or Simplified – as listed in art. 9d and 9i, or Extended – as described in art. 9e. Due diligence is the tool of detection of any symptoms of money laundering at the beginning of the relationship. KYC is described in art. 7 and 8 of the Directive and implemented in art. 8b of the Polish AML Act. Due diligence is the customer identification to such extent that we understand its business structure, ownership structure, transaction profile and management quality. Cases when due diligence has to be performed are: establishing the relationship, carrying out the occasional transaction over EUR 15,000 in a single or in several linked transactions, a suspicion of money laundering and the doubts about the accuracy of the customer identification data.

2.2. Due diligence based on a risk-sensitive basis means that for some customers we need to collect much information but for other, "less risky", we do not have to check almost anything. It also means that covered institution can decide of the extent of its measures of weighting the risk and these measures are not the same for all covered institutions. The examples of the obligation to apply the enhanced due diligence are Politically Exposed Persons and Correspondent Banks from third countries – art. 9e of the Polish AML Act and art. 13 of the Directive. The simplified due diligence is acceptable for customers being covered institutions in the EU and third countries, which imposes equivalent AML requirements and publicly traded companies. All obtained customer identification data including the beneficial owner have to be verified before the establishment of a business relationship or carrying out of the transaction but in some cases it can be done as soon as practicable after the initial contact.

2.3. One of the significant elements of due diligence – ongoing monitoring of processed transactions – is mentioned twice in the Polish AML Act: art. 8a and art. 8b item 3.4. One aspect of monitoring refers to ensure that conducted transactions are consistent with the customer business model, which is strictly connected to "Know Your Customer" concept. Second aspect (art. 8a) is related to current analysis of conducted transaction and requires that the results of the analysis are documented. The difference between these two aspects of monitoring transactions is not explored

enough at this moment and probably will be the subject to the FIU interpretation in the future.

2.4. The Directive (art. 13) and Polish AML Act prohibit covered institutions from entering into correspondent banking relationship with shell banks (art. 9f) and opening of anonymous accounts. Such account when existing shall be terminated or disclosed within 12 months – art. 19. The covered institutions shall take special due care when dealing with products which support anonymity.

2.5. Polish AML Act introduced the separate paragraph 5a – "Special means taken against persons, groups and entities". This is the response to FATF regulations related to international sanctions. This area was not regulated in the local legislation and the financial institutions, including Citi Handlowy, performed the sanctions screening basically on corporate regulations of Parent Company. Paragraph 5a delegates to the Ministry of Finance the obligation to publish the list of sanctioned persons, groups and entities. Based on this list, covered institutions have to freeze the funds of sanctioned person if they are the participant of the transaction. According to the Polish Banks Association, there is too weak protection against the consequences of such decision for the covered institutions. The practice in the subject will be thoroughly observed by the banks representation.

3. Adjustment of the internal procedures

All new provisions of new AML Act should be implemented by covered institutions in the form of internal procedure describing the individual approach to prevention of money laundering and its own measures of all risks related. In accordance with art. 10a (art. 34 of the Directive) the procedure shall describe as follows.

3.1. Customer due diligence process. In Citi Handlowy the policy was implemented a few years ago as a corporate policy introduced by the US Parent Company further to FATF regulation. The method of performing due diligence is Customer Application Due Diligence (CADD). The relationship team has the obligation to prepare CADD for each new customer. CADD is prepared based on documentation and the interview with the customer. At least one visit is obligatory before the bank enters into relationship. The required documentation consists of the deed of incorporation of the customer, statutes, by-laws, an updated excerpt from KRS or issued by the competent registration authority of the country in which such foreign customer has its seat. The collected documents have to be in original or certified by a notary or Polish consular office for non-residents. Additionally to the above information there is the obligation to identify the members of the entrepreneur's corporate bodies and all representatives, their names, addresses and numbers of identity cards/passports. Having the personal data of the representatives it is necessary to check these data with the sanction lists. Any "match" with the sanction list is to be consulted with the Compliance Officer in the bank. Depending on the type of "match", the Compliance Officer takes the decision to enter into relationship or not. The entirely new element

which has to be adopted into current internal procedure is the duty to identify the beneficial owner in order to understand the ownership and structure of the customer.

3.2. Very important element of due diligence is preparation of the account profile of the customer. This is a form dedicated to describe which product will be offered to the customer and what the purpose of the account is. It also contains the estimated turnover on the account.

3.3. Risk assessment model. This model is based on three categories which are subject of assessment:

a) entity risk – private or public company, institution type (pension funds or military manufacture), Publicly Exposed Persons involved,

b) geographical risk where the customer has its seat or is registered ("tax haven" or sanctioned countries),

c) product or transaction type which the customer is interested in (export Letters of Credit or local settlement with buyers and sellers).

When all information is entered into risk model the total point score shows the risk level linked to this relationship. Three levels of risk are used: low, medium and high risk.

The file of CADD, Account Profile and Risk Assessment is subject to periodical revision to observe any potential changes in the customer behaviour and status. The frequency of the revision depends on the risk involved. For low risk customers the review is once every 3 years, for medium risk – every 1.5 year, and annually for high risk customers.

3.4. Reporting obligations and record keeping. Each covered institution has to report any transaction which seems to be money laundering or terrorism financing in order to prevent using this institution for the criminal actions. The procedure of the reporting of suspicious transactions shall describe:

a) the unusual patterns which are the subject of searching,

b) the system of communication within the institution and the designated person who is authorised to report the problem to the regulatory.

It means that the staff processing the transactions has to be aware and prepared to recognise the symptoms before the transaction is passed and to deliver the alert to the next level of the chain. Such manual model can work for large and complex transactions which are processed manually but it is impossible to monitor manually mass of transactions in the large institution like Citi Handlowy. The method of identification of suspicious patterns has to be automatic or semi-automatic and performed on a large population of transactions. The population of transactions is built from all daily transactions recorded in the Register of Transactions. If we define in advance the rules for searching the population, we can expect the daily report of transactions which met the rules and should be explored further manually. In order to automate the selection of unusual transactions Citi Handlowy uses Citigroup Anti-Money Laundering Business Rule Standards – CAMBRS. It is the list of situations which have been defined as potentially problematic from money laundering perspective.

The examples of such standards are "rapid movement of funds" or "hidden relationships". The number of standards depends on the institution and its experience. The most important is that the standards identify patterns and behaviours which can be the symptoms of placement, layering or integration of funds. The next step of the process is the analysis of all transactions meeting the rules and presented as the exceptions. This stage is based on "Know Your Customer" procedure. Each potentially problematic transaction is then revised against the customer pattern of transactions and the business model. Relationship managers, who know their customers, participate at this stage of the analysis and give the advice if the situation is in line with the customer standard business way or not.

Depending on results of the analysis, the transaction can be reported to FIU by the designated officer from the institution.

In addition to "case by case" reporting, Polish FIU demands the periodical reporting of all transactions over EUR 15,000 or less if they were divided intentionally to avoid the registration. The structure of the report is strictly defined and requires the support of professional IT system for the institutions with large volume of transaction. The internal procedure shall describe the process of uploading the system, searching for unusual patterns and generate the report to FIU. Article 30 of the Directive and art. 8a of the Polish AML Act requires that the documents and information evidenced the due diligence and transaction monitoring need to be kept for a period of 5 years following the carrying-out of the transactions or the end of the business relationship. It means that the system recording this information needs to be archived and data should be accessible for the required period.

3.5. Internal controls. An internal procedure should describe the frequency and method of internal controls over the process. The most important is to designate the person who is responsible in the institution for the avoidance of money laundering and terrorist financing and is authorised to contact the government supervision. Apart from this, there should be dedicated unit of independent internal control appointed for performing the overview of the whole process. Control methods can be periodical reviews of part of process or end-to-end reviews, monitoring of statistics measuring the efficiency of the detection process, self-assessment of key risk indicators defined by the institution. One of the examples of key risk indicators can be the number of periodical due diligence which were not executed on time or number of exceptions not answered on time.

4. Potential problems in the implementation

4.1. One of the most difficult and widely discussed subjects in the new AML Law is the beneficial owner. Who is the beneficial owner? The definition (art. 3 of the Directive and art. 1a in the Polish AML Act) is quite long but to simplify we can divide it into three categories:

a) natural person being direct owner or controller over the customer,

b) natural person being shareholders in the legal person having 25% of voting rights,

c) natural persons having the control over 25% of assets in the entities that administers or distributes funds like trusts, foundations.

In very complex structures of some legal persons where the shareholders or the direct owners are legal persons too, the covered institution may have no instruments to find out the beneficial owner. The legal person who is the owner of the customer is not our customer and the access to the information of its structure is limited to those publicly known, but they are very limited and not sufficient. In some cases, when the shareholders are registered in the company's book only, we cannot even ask for the owner's name.

Hopefully, art. 8b requires an identification of the beneficial owner WHENEVER APPLICABLE. In many cases, it will not be applicable. For Polish customers and its owners/shareholders the institutions can use electronic KRS, Panorama Firm database, information from local and government administration, General Statistical Office (GUS). For legal persons registered outside Poland it can be Word Check or different commercial databases. For customers using financing it can be Coface[3] or similar organizations.

4.2. The proposed structure of the Register of Transactions. The Ministry of Finance published the project of changes to the structure of the Register of Transactions. Proposed Chart of transaction might become the mirror of all information collected by covered institutions during the due diligence process. Current scope of the Chart is already complex and exceeds the scope of information sent with the transfer of funds transaction. The information-like legal form, the number of the companies' register, tax identification number, citizenship, PESEL, the number of the identity card, are not included in the transaction content. The plan of MF to extend evenly the scope of Chart of transaction with the beneficial owner details raised the protests from banking industry. In accordance with the Directive the only purpose to gather the information of the beneficial owner is to understand the ownership structure of the customer and assess the risk related to this and there is no reason to attach this information to every single transaction. Moreover the information of the beneficial owner is not always applicable while the respective tag in the Chart of transaction tends to be obligatory. It may happen that the covered institutions will be forced to demand from the customer more information than necessary, which may be the source of potential dissatisfaction of the clients. Expenses are not neutral for the covered institutions. The necessity of transferring the customer identification data recorded in the main systems and attaching them to the single transaction in the Register of Transactions requires the huge IT investments in software and hardware. It is expected in banking environment that the discussion on this subject will be continued.

[3] A worldwide credit information and credit insuring company.

4.3. PEP[4] identification and due diligence requirement is widely discussed among the covered institutions. The definition of Publicly Exposed Person covers not only the prominent political officials but also their relatives and associates. The decision to appoint somebody as PEP is quite judgmental and based on media information. The reasonable adoption of this requirement is to solely act on publicly known information without having any extended investigations. Very helpful in this task are commercial databases like World Check and other similar. When the customer is PEP, the extended due diligence is to be applied. The Polish AML Act excluded Polish PEP from this classification while the Directive does not mention the residence place of PEP as a condition to classify or not.

4.4. Article 9d applies the simplified due diligence in the following cases:

a) the customer is a credit or financial institution covered by the Directive or situated in a third country which imposes regime equivalent to those laid down in the Directive,

b) the customer is listed company on the regulated market,

c) the customer is the domestic public authorities,

d) some types of the life insurance,

e) some types of the insurance policies linked with pension.

According to item 3 of this article, covered institution has to gather the information to establish if the customer qualifies for the exemption. This is imposed in the Directive and in the Polish AML Act as well. It seems that simplified procedure can be difficult to apply because gathering information and documents means performing a due diligence process. Moreover, nobody knows today what kind of information should satisfy the regulatory that the customer is exempted. Probably the market practice or FIU interpretation will be required in the future.

5. Technological support and changes of the existing IT systems

5.1. IT Systems used by the covered institutions need to be adjusted to the new requirements. In any time the institution has to know which customer is classified as PEP in order to apply enhanced due diligence and put the customer into high risk group. The system, in which the customer base is kept, needs to be uploaded with new information – PEP. According to this information the institution will be able to report to the regulatory all its PEPs list if required. Additionally the covered institutions have to choose the source which will be used for searching PEPs and sanctioned persons. There are commercial databases accessible on the market. The decision depends on the cost level acceptable by the covered institution. Without any doubts PEP and sanction searching requires IT investment.

5.2. In accordance with the art. 17, covered institutions have to review all customers within 12 months and perform the risk assessment of every single customer.

---

[4] Politically Exposed Person.

The risk level has to be marked in IT system keeping the customers' base. The "risk level" parameter is necessary as the factor determining due diligence scope. There are many methods of risk classification; the sophisticated models are available on the market provided by the advisory and accounting auditors but the most simple risk classification is 3-level model: low, middle and high risk. From IT system perspective we need to have at least 3 parameters in IT system.

5.3. As a result of risk classification, the respective due diligence scope is determined. The scope of due diligence can be normal, simplified and enhanced and each of them should be described in the internal procedure. Normal due diligence is in the provision of art. 8b of the AML Act. It covers 4-point checking: customer identification, beneficial owner identification, the purpose and nature of business, and ongoing monitoring of the customer activity. For some type of customers, being by definition low risk institutions, we can apply simplified due diligence and refrain from application of some elements of due diligence, which is specifically described in art. 9d and 9i. For other types of customers, being by definition high risk institutions, we must apply the enhanced due diligence (art. 9e). From IT system perspective we need to have the possibility to define the scope of due diligence and the frequency of periodical review by using new system parameters.

5.4. By applying the due diligence means, we receive an entirely new information – beneficial owner's identity. This information is to be recorded in the system and updated once the identity is changed. We insert this information in the "customer maintenance" module of the system in order to have the possibility to transfer this information to the Register of Transactions. Depending on structure of the system used by the covered institution, it requires more or less complicated re-engineering. Especially, the interface transferring data from operational system into the Register of Transactions must be enhanced.

5.5. Another task to do in order to implement new requirements is to select customers whose transactions should not be registered any more. In art. 8 item 1e point 6 there is the exemption from registration of transactions related to the customers:

a) being the institutions providing the financial services in EU or third countries, which imposes equivalent AML requirements,

b) being the government or local administration.

Such types of customers have to be marked in the "customer maintenance" module of the system. The transactions initiated by customers with "N/A" parameter should not be transferred into the Register of Transactions. This task seems to be simple but in practice it is really complex and manual process. The covered institutions never classified customers in such a way. Existing classification used in financial reporting or National Bank of Poland reporting does not match exactly those criteria implemented by AML Act. It requires practically the manual checking of the documents of each customer and classifying them one by one in accordance with above criteria.

6. Conclusions

The implementation of the Directive 2005/60/EC on the prevention of the use of the financial system for the purpose of money laundering and terrorist financing into Polish legal system has lasted more than 3 years. From Citi Handlowy perspective, being the active member of the consultation since 2007 as a member of Polish Banks Association, it was time spent on very interesting discussions with the Ministry of Finance and GIIF. The aim of these discussions was to explain the difficulties in proper execution of the regulations and to convince the regulatory of simplification of the prevention system wherever possible. The difficulties could be limited by adequate protection of covered institutions and their employees, an access to governmental database, simplification of very developed system of registration and reporting. In 2008 covered institutions registered and sent to GIIF 34.8 billions of transactions. In order to keep and process such huge number of transactions, the strong IT investments were required at covered institutions and GIIF side. On the other hand, GIIF informed of blocking 319 accounts and sending 246 cases to the prosecutor. In 2008 the courts sentenced money laundering in 27 cases.

As a result of amendment of AML regulations, banks and other covered institutions have to reengineer internal procedures and make further investment in technology infrastructure. If the system of registration of transaction is simpler, with less data, this would be achieved at reasonable costs for all. Nobody has doubt that development of methods and measures protecting from money laundering and financing of terrorism is necessary not only due to regulations requirements but also in order to protect the reputation risk of covered institutions.

References

GIIF report of the execution of AML Act in 2008, www.mf.gov.pl.

The Directive 2005/60/EC of the European Parliament and of the Council of 26 October 2005 on the prevention of the use of the financial system for the purpose of money laundering and terrorist financing, *Official Journal of the European Union*, 25.11.2005, L 309/15, http://www.infor.pl/dzienniki-unii-europejskiej,seria-L,rok,2005,nr,309.html.

The Act of 25 June 2009 amending the Act on counteracting introduction into financial circulation of property values derived from illegal or undisclosed sources and on counteracting the financing of terrorism, *Dziennik Ustaw* [Journal of Laws] Nr 166, poz. 1317, 2009, http://lex.pl/serwis/du/2009/1317.htm.

Unpublished consultative comments letters of Polish Banks Association.