Personal Identification in Financial Services

Irmantas Rotomskis[1]

Marius Laurinaitis[2]

Abstract. **The article analyses how financial institutions in Lithuania identify their customers before starting to provide their services to them, and how the mentioned institutions implement the principle "get to know your customer." This requirement has emerged from the importance of the prevention of money laundering. In the complex legal regulatory mechanism the following concepts appear: proper identification, simplified identification, identification without being physically present. These methods differ with regard to the scope of the gathered personal data and the method of data collection. Theoretical legal possibilities not to gather personal data appear where customers can stay anonymous in electronic payments of small sums especially in the case of electronic money.**

Index Terms: **prevention of money laundering, customer identification, customer due diligence measures, simplified customer due diligence measures, enhanced customer due diligence.**

JEL Classification: **G2, K33, K4.**

I. Introduction

Identification of customers of financial institutions is a fundamental element of internal control of these institutions. Identification is necessary in order to protect financial institutions from risks such as abuse, fraud, operational, business reputational and strategic risks. But most often customer identification is related to requirements established in legal acts in order to prevent possible money laundering and terrorism financing. For a long time the most popular and the safest method to hide taxes and to possibly launder money was anonymous accounts. With the help of these accounts it was possible to hide illegally received money. Fighting against money laundering and terrorist financing, EU Member States adopted the Directive 91/308/EEB on the prevention of the use of the financial system for the purpose of money laundering, where it was indicated for the first time that Member States must forbid their credit and financing institutions to have anonymous accounts or anonymous passbooks (COUNCIL DIRECTIVE 91/308/EEC). Currently based on this Directive EU Member States have already renounced anonymous accounts.

The decision to establish the Financial Action Task Force on Money Laundering (FATF) made in 1989 by the G-7 Summit increased the transparency of financial institutions. The main areas of activities of FATF were the fight with shadow economy and observation of tendencies and technologies. In 1990 FATF passed the Forty Recommendations for fighting against money laundering. In 1996 the Recommendations were reviewed for the first time because of technological changes in the activities of money laundering due to the appearance of electronic payments and the use of these technologies in the schemes of money laundering. The 1996 Forty Recommendations have been endorsed by 130 countries and have become the international standard for money laundering prevention. These Recommendations were transferred to the first EU Directive on money laundering prevention. This article will analyse the Recommendation No. 5 in depth (FATF 40) ("Financial institutions should not keep anonymous accounts or accounts in obviously fictitious names. Financial institutions should undertake customer due diligence measures, including identifying and verifying the identity of their customers".), giving the most attention to the discussion of customer due diligence measures existing in Lithuania. This article will analyse the provision of contemporary financial services by electronic means and customer identification procedures in physical as well as cyber space. The changes of legal acts adopted in Lithuania in 2013 allowed financial institutions to start business relationships with customers without them being physically present with the help of qualified certificates. Why qualified certificates? Why a safe electronic signature, which can be substituted by electronic identification systems of third parties (banks), is not sufficient? Also the practice when fast loans companies cannot identify their customers through banking systems and cannot start business relationships – ant collect private data – is an especially relevant topic.

II. Current State and Theoretical Background

a. Definition of customer identification

We use our personal information every day, we depend on it, it identifies us. Identification is also necessary where our physical participation is impossible – i.e. in cyberspace. We provide our personal data when connecting to financial services, seeking to use electronic banking services, electronic money, etc. The information that identifies us differs in physical and cyber spaces – other requirements are raised for this information. (Štitilis, Pakutinskas, Dauparaitė, Laurinaitis) When seeking to confirm our identity in physical space, we do this using one of the obligatory elements – an identification document. IDs follow us through our whole life; they are obligatory to have for people living in Lithuania as well as other countries. Identification documents issued by the state form a person's identity – a legal identity of person. The most important legally recognized documents that

[1, 2] Irmantas Rotomskis and Marius Laurinaitis are with the Faculty of Economics and Finance Management, Mykolas Romeris University, Lithuania.

confirm personal identity in physical space most often are identity cards and passports. Such documents are provided only by institutions authorised by the state, and they are the only legal identification means. (Štitilis, Pakutinskas, Dauparaitė, Laurinaitis) Financial institutions have been assigned the function to duly identify their customers in physical space, but are they capable of doing this? A practice has formed that identification in physical space with the customer being physically present is more secure than identifying the customer remotely. This practice is characteristic of many European countries. And supervision institutions check identification processes and received personal data of customers of financial institutions especially thoroughly.

All financial institutions must identify their clients and benefit recipients (Law 22 December 2011). Most often this requirement is applied before business relationships are started. It is necessary to emphasize that one-off operations are not considered to be business relationships if they do not exceed the set limits. Business relationships suppose constant cooperation with a financial institution. Financial institutions, observing regulation in physical space, identify people with corresponding measures. (Resolution No. 942) In Lithuania the application of these measures and the related procedures are indicated in a separate Resolution of the Government (Resolution No. 942). As foreseen in the Law of the Republic of Lithuania on the Prevention of Money Laundering each financial institution chooses the method used for identification: a due/full or a simplified one. In the framework of our analysed subject we will discuss only these methods and exceptions related to payments in physical and cyber space. Legal acts foresee that identification is performed only with the customer being physically present (exceptions and order when a customer can be represented by another person are also provided). It is indicated that when starting customer identification an employee of the financial institution must assess whether the customer provides a valid identification document and to determine if the provided document contains a photograph of the customer (Resolution No. 942). The regulator – the state – foresees the duty to identify, but does it create some real means to do this? It should be emphasized that the primary function of financial institutions is not identification or implementation of the prevention of money laundering. Financial institutions seeking to properly implement functions given to them by the state must finance the operation of these procedures themselves, i.e. if an employee must assess if the document presented is valid, s/he has to have the possibility to do this. The validity of the document is determined based on the data of the public registers but in order to ascertain the authenticity of the data on the document it is necessary to order special extracts from state registers, which incurs additional costs. Another interesting moment is the requirement to determine that the presented document contains a photograph of the said customer. What means can be used for this aim? Only visual contact? People change with time; sometimes these changes are significant, so external characteristics alter. The necessity of such requirements and factual problems encountered by employees of financial institutions do not allow proper implementation of the mentioned requirement. Let us take a simple example: would an employee of a financial institution in Lithuania be able to vouch that the photograph of a Chinese citizen or of an immigrant from Nigeria presented to them belongs to the person standing in front of them? Such requirement is understandable but before setting the regulatory mechanism it is necessary to make it clear how financial institutions will be able to implement it. It is necessary to keep in mind that they do not have to perform the functions of the state. Similar problems are related to another practical requirement to assess the state of the presented document (Resolution No. 942). It is difficult to ensure that employees of financial institutions were also document specialists. If the document has been professionally altered, if the photograph in it has been changed, it is impossible for a simple employee to distinguish this. This method of identification in physical space is practically applied uniformly in all countries of the European Union. EU countries have implemented the provisions of the Directive on the prevention of the use of the financial system for the purpose of money laundering and terrorist financing of 2005 (Directive 2005/60/EC). The Directive of 2005 introduced new identification concepts such as customer due diligence measures and simplified customer due diligence measures. Customer due diligence measures (identification) are used most often and applied before the start of business relations. Simplified customer due diligence measures encompass simpler standards when identifying customers.

We will discuss in more detail the method of simplified customer due diligence measures for electronic payment systems in Lithuania. All banks in Lithuania identify their customers duly and practically they do not apply the simplified identification therefore we will analyse customer identification procedures of other financial institutions – institutions of electronic money. The Directive of 2005 (Directive 2005/60/EC) as well as Lithuanian legal acts (Law 22 December 2011) in the case of electronic money allow to apply simplified customer due diligence measures, indicating that this is valid for electronic money, if the device cannot be recharged, the maximum amount stored in the device is no more than EUR 250, or where, if the device can be recharged, a limit of EUR 2500 is imposed on the total amount transacted in a calendar year, except when an amount of EUR 1000 or more is redeemed in that same calendar year by the bearer (Directive 2005/60/EC). The indicated sums are small therefore the risk that it will be used for money laundering is small. It is logical to think that this would also allow applying easier identification methods, as indicated in the name “simplified customer due diligence measures”. But when analysing the regulatory mechanisms in Lithuania it becomes clear that electronic money issuers must identify their customers properly even though they qualify for the exception described in the law. The mentioned Resolution of the Government of Lithuania (Resolution No. 942) indicates that when applying simplified customer due diligence measures financial institutions can choose a

corresponding point from the indicated methods for customer identification. But almost all methods that can be chosen talk about physical participation of the person during identification, about the necessity to make a copy of the person's personal identification document, and in the case of electronic money, especially in online based electronic money systems, such requirement becomes unrealisable. The purpose of electronic money is to ease the transmission of value. When talking about electronic money of low value and about the applicable sum limits (Directive 2005/60/EC) there is even a possibility to be an anonymous user. Such small value payment means are often used by children but in Lithuania an imperative regulatory mechanism exists that foresees that identification is necessary even in the case of small values in case of electronic money.

b. Electronic customer identification

Up till the middle of 2013 financial institutions in Lithuania did not have a legal possibility for customer identification based on their present electronic identity, although a qualified electronic signature is issued by several providers in Lithuania. (We will not discuss electronic signatures or their types in this article; we will talk only about its application in the financial sector for identification procedures.)

The possibility to identify customers remotely existed also before 2013. The Directive of 2005 (Directive 2005/60/EC) described the possibility when a person could act through his/her representative. If transactions or business relations are made through a representative or the customer is not physically present during his/her identification, or when there is a big risk of money laundering and (or) terrorist financing, financial institutions and other subjects must apply enhanced customer due diligence identification measures (Law of the Republic of Lithuania on Prevention of Money Laundering). During enhanced identification it is necessary to use additional means. It is necessary to use additional data, documents or information for customer identification and also to use additional measures for verification or confirmation of presented documents. Based on these rules it is not possible to transmit only a simple copy of the document electronically (to send a scan of it) because it will not be possible to verify or confirm the presented documents. A possibility is foreseen that another financial institution can do this by presenting a certificate that confirms the customer's data (the so-called third reliable party that identifies and verifies the identity and transmits the fact to another financial institution). Another foreseen measure is that the first payment would be performed through the account opened in a credit institution in the customer's name, which would allow to verify if the customer's presented data correspond to the data of the sender indicated in the bank transfer. It is necessary to emphasize that these means are applied together, i.e. by using the enhanced identification the financial institution must receive as much data as possible that would allow to confirm the identity of the customer.

In August of 2013 the mentioned Resolution of the Government of the Republic of Lithuania (Resolution No. 942) was supplemented, identification procedures were expanded and next to proper identification a possibility appeared to identify a person without the customer being physically present. "The financial institution or another entity may identify customers, who are citizens of the Republic of Lithuania without them being physically present, i.e. remotely, using a qualified electronic signature and only in cases when the customer's identity, before issuing a qualified certificate to him, was identified with him being physically present" (Resolution No. 942). This new norm allowed what had been not allowed before – to properly identify a customer's identity based only on a valid qualified electronic certificate. Until the appearance of this norm no financial institutions were allowed to do this in Lithuania. An electronic qualified certificate is accepted as a legally valid identity document in cyberspace (Law of the Republic of Lithuania on electronic signature). And all documents or public services of state institutions in cyberspace[1] are provided using the identification method adapted to cyberspace – an electronic signature. But a strange discrepancy appears. Lithuanian state institutions use an electronic certificate when they identify citizens/customers, but it is not necessarily qualified, i.e. customers are free to choose the method of identification, and often they choose the method that is the most widely spread currently: identification using a reliable third party – a bank. Electronic banking services use their identification system that joins two elements of identification in cyberspace: what they know and what they have (Štitilis, Pakutinskas, Dauparaitė, Laurinaitis). The security means used by a bank to identify customers are identification codes, passwords, password cards, and password generators. A customer chooses the recognition means provided to the user him/herself (Štitilis, Pakutinskas, Dauparaitė, Laurinaitis), and based on the legal regulation such method of identification and such security measures can become a secure electronic signature (Law of the Republic of Lithuania on electronic signature). But such signature is not qualified because qualified electronic signatures can be issued only by electronic signature providers accredited by supervision institutions (Law of the Republic of Lithuania on electronic signature). Customer authenticity is considered to be confirmed if the user has used the recognition and security measures provided by the bank correctly and if the bank has received the user's information about his/her registration in the system. The bank acknowledges this identification system as an electronic certificate, and it considers all confirmed documents to be equivalent to written ones. Such possibility is given to banks by the Law on electronic signature (Law of the Republic of Lithuania on electronic signature): customer identification systems for electronic data used by banks have the same legal power as a signature on written documents and are admissible as proof in court in all cases because the customer and the bank have mutually agreed so. Practically the identity created by banks corresponds to the

1 E-Government Gateway: https://www.epaslaugos.lt

real personal identity because banks use the most important principle of proper customer identification but our legislators have chosen only the qualified electronic certificate as the possibility for remote identification. Such strict position creates many inconveniences: many consumers have banking means, i.e. they have already been duly identified so why shouldn't it be possible to use them if they need to identify themselves in another financial institution? We believe that the principle of technological neutrality is violated in this way.[2] This concrete requirement – to use qualified certificates – created a big wave of problems for providers of fast credits in Lithuania, who allowed to sign agreements of credit reception remotely using electronic banking systems. Supervision institutions in Lithuania penalised several fast credit companies. Legal proceedings are still going on but the essential argument of the court is that legal acts on the prevention of money laundering foresee that if the identity is determined without physical participation the enhanced identification procedure should be applied automatically or a qualified electronic signature must be used whereas credit transfer using electronic banking is not considered to be a proper means of enhanced identification.

Another important question is why only citizens of the Republic of Lithuania can use qualified certificates when starting business relations in Lithuanian financial institutions remotely? Is that not a discrimination of EU citizens? Because qualified certificates, issued in EU countries, are valid and have legal power in all EU countries (Law of the Republic of Lithuania on electronic signature). So citizens of other countries, who have a qualified certificate, issued in the EU, and who want to open an account in a bank in Lithuania remotely, will not be able to do that. This all looks strange knowing that Lithuania participates in the project of unified identity in the EU STORK[3] - the main aim of the project is the possibility for EU citizens to use their electronic identities in all EU countries.

III. Empirical research

We will discuss concrete examples in Lithuania. We have chosen active institutions of electronic money as our object because commercial banks and other big financial institutions in Lithuania theoretically perform proper customer identification. Currently two companies have licences to issue electronic money in Lithuania (Electronic money institutions). One of the companies is ANTIGRAVITY PAYMENT SYSTEMS; they have a licence for restricted activity, and they can operate only in Lithuania. Another company – EVP International – has a licence to operate in the whole EU. These companies directly encounter problems of remote identification.

ANTIGRAVITY PAYMENT SYSTEMS owns the brand MokiPay, which is a platform of mobile payments that allows customers to perform payments in physical space using their mobile phones or contactless cards. Their services are financial services therefore their customers must identify themselves. The exception discussed above relating to electronic money regarding simplified identification is valid, but customers have to provide a part of their data, and anonymity is not possible in practice. But when analysing the agreement between consumers and *MokiPay* a point allowing anonymity can be found: "*4.4.The following limits shall be set for the Clients **who have not identified themselves** according to the procedure established by the laws: the total value of payment transactions during a calendar year may not exceed LTL 8,500, the amount of money kept in the MokiPay Wallet at any time may not exceed LTL 500, and the amount per payment transaction may not exceed LTL 500. The Clients who have identified themselves according to the procedure established by legal acts may keep more than LTL 500 in their MokiPay Wallets and the total amount of settlements per year may exceed LTL 8,500."(*Antigravity payment systems) Basically *MokiPay* allows their customers to be anonymous in small payments, and that is good, but an imperative prohibition exists in laws, so how can it be that laws prohibit, and the subject operates? We believe *MokiPay* operates legally because firstly we have to see the system's aim and purpose. If an anonymous user can operate only with small sums, if s/he can pay small sums and transfer them to another user of *MokiPay*, practically there is no risk of money laundering. The risk appears if money were exchanged back to cash, but in this case *MokiPay* foresees strict measures and identification. So it is impossible to stay anonymous if customers wish to exchange their electronic money for cash or if customers plan to take their money out of the *MokiPay* system. Such measures adopted by *MokiPay* really ensure proper prevention of money laundering, and it would really be disproportionate to require each customer, who uses this means to perform micro payments, to identify him/herself. *MokiPay* has all the necessary means for proper customer identification; customers may use their qualified electronic signatures seeking to become customers of *MokiPay* and to operate with bigger sums of money without restrictions (Antigravity payment systems).

Another company of electronic money (the biggest one in Lithuania) is EVP International, managing brands *mokejimai.lt* and *Paysera*. It does not leave any practical possibility for its customers to stay anonymous. This situation is explained by the fact that this company is an online based money creator, and customers can exchange this kind of money freely in Europe and beyond, therefore the risk is bigger. All customers of this company have been duly identified (General payment service agreement).

The purpose of electronic money is everyday small payments. The Directive on electronic money of 2009 (Directive 2009/110/EC). transferred into the Lithuanian

2 The principle of technological neutrality states that the state cannot establish a dominating technology by legal acts. It can only set minimal requirements for it.

3 The aim of the STORK project is to establish a European eID Interoperability Platform that will allow citizens to establish new e-relations across borders, just by presenting their national eID. Cross-border user authentication for such e-relations will be applied and tested by the project by means of five pilot projects that will use existing government services in EU Member States. In time however, additional service providers will also become connected to the platform thereby increasing the number of cross-border services available to European users. https://www.eid-stork.eu/

legal system (Law of the Republic of Lithuania on electronic money and electronic money institutions), gave a start to the appearance of new financial institutions in Lithuania, thus raising many new problems related to customer identification.

Electronic money seeks to change cash in everyday payments; both adults and children want to use it, but legal regulation does not make a difference regarding to this and indicates to identify, and the means to perform this are really difficult and sometimes are not even accessible for children (electronic qualified signatures).

Europe understands the importance and potential of electronic money and plans to change the requirements regarding identification in the new Directive on the prevention of money laundering that has not been adopted yet (Law of the Republic of Lithuania on electronic money and electronic money institutions):

Member States may decide to allow obliged entities not to apply certain customer due diligence measures in respect of electronic money, if all of the following risk mitigating conditions are fulfilled:

(a) the payment instrument is not reloadable;

(b) the maximum amount stored electronically does not exceed EUR 250. Member States may increase this limit up to EUR 500 for payment instruments that can only be used in that one particular Member State;

(c) the payment instrument is used exclusively to purchase goods or services;

(d) the payment instrument cannot be funded with anonymous electronic money;

(e) the issuer carries out sufficient monitoring of the transactions or business relationship to enable the detection of unusual or suspicious transactions.

But this future Directive also leaves the right to Member States to decide if identification should be applied or not. Who will guarantee that countries will not choose the more complicated version thus distancing us from modern payment means? The regime of the prevention of money laundering for institutions of electronic money applied in Lithuania is one of the strictest in Europe, so there is no sense in talking about stimulating the competition. The biggest institutions of electronic money in Europe can identify new customers based on a reliable third party – a bank: it is sufficient to relate the payment card with the account of electronic money, and such method of identification is sufficient. Therefore often many customers choose the simpler way – because simplicity leads to massification.

IV. Conclusions

The main purpose of the article was to reveal the procedures of identification in Lithuania. Each financial institution in Lithuania must identify its customers before starting business relations.

Identification procedures described in legal acts in force in Lithuania encompass due, simplified and enhanced identification methods.

Financial institutions have a new possibility to start business relationships with customers using electronic qualified certificates.

The possibility foreseen in Lithuanian legal acts to use qualified certificates for identification in the financial sector only for citizens of the Republic of Lithuania violates EU consumer rights and distorts competition.

The regime of the prevention of money laundering for institutions of electronic money applied in Lithuania is one of the strictest regimes in Europe; the possibility for underage persons to use such money freely and comfortable hasn't been thought of at all. All potential risks are really small therefore identification requirements for electronic money of small value could be significantly decreased.

The state seeking for a 'society without cash' should create certain legal provisions instead of burdening low risk financial services with strict identification requirements.

References

Council Directive of 10 June 1991 on prevention of the use of the financial system for the purpose of money laundering (91/308/EEC).

FATF 40 and IX Recommendations. The revision of the FATF Recommendation was adopted and published in February 2012. [Online] Available: http://www.fatf-gafi.org/media/fatf/documents/FATF%20Standards%20-%2040%20Recommendations%20rc.pdf [Accessed: May. 5, 2014]

Štitilis D., Pakutinskas P., Dauparaitė I., Laurinaitis M. Preconditions for Legal Regulation of Personal Identity in Cyberspace // Jurisprudencija, 2011, Nr. 18(2), p. 703-724. ISSN 1392–6195 (print), ISSN 2029–2058 (online).

Law of the Republic of Lithuania on Prevention of Money Laundering and Terrorist Financing, as last amended on 22 December 2011 – No XI-1885.

Resolution No. 942 of 24 September 2008 on the List of criteria for considering a customer to pose a small threat of money laundering and/or terrorist financing and criteria based on which a threat of money laundering and/or terrorist financing is considered to be great, On the approval of the rules of customer and beneficial owner identification as well as detection of several interconnected monetary operations, and on the establishment of the procedure of presenting information on the noticed indications of possible money laundering and/or terrorist financing and violations of the Law of the Republic of Lithuania on prevention of money laundering and terrorist financing as well as the measures taken against the violators.

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.

Law of the Republic of Lithuania on electronic signature, July 11, 2000. No. VIII – 1822, amended as of June 6, 2002. No. IX – 934.

Electronic money institutions. [Online] Available: http://www.lb.lt/electronic_money_institutions_1 [Accessed: May. 5, 2014]

"Antigravity payment systems" agreement for payment and regulations [Online] Available: http://www.mokipay.com/en [Accessed: May. 5, 2014]

General payment service agreement. [Online] Available: https://www.paysera.com/terms_and_conditions.html [Accessed: May. 5, 2014]

Directive 2009/110/EC of the European Parliament and of the Council of 16 September 2009 on the taking up, pursuit and prudential supervision of the business of electronic money institutions amending Directives 2005/60/EC and 2006/48/EC and repealing Directive 2000/46/EC (Text with EEA relevance)

Law of the Republic of Lithuania on electronic money and electronic money institutions 22 December 2011 No XI-1868

Proposal for a Directive of the European Parliament and of the Council on the prevention of the use of the financial system for the purpose of money laundering and terrorist financing.