INDEPENDENT JOURNAL OF MANAGEMENT & PRODUCTION (IJM&P)
http://www.ijmp.jor.br *v. 12, n. 3, Special Edition ISE, S&P - May 2021*
ISSN: 2236-269X
DOI: 10.14807/ijmp.v12i3.1532

DISTANCE PERSONAL IDENTIFICATION IN THE ON-LINE ENVIRONMENT: PROBLEMS OF FINANCIAL INSTITUTIONS IN THE EU

Marius Laurinaitis
Mykolas Romeris University, Ukraine
E-mail: mariuslituania@ukr.net

Darius Stitilis
Mykolas Romeris University, Lithuania
E-mail: stitilis@mruni.eu

Irmantas Rotomskis
Mykolas Romeris University, Lithuania
E-mail: irotom@mruni.eu

Oksana Novak
Zhytomyr Polytechnic State University, Ukraine
E-mail: novak_os@ukr.net

Oleksii Lysenok
National University of Food Technologies, Ukraine
E-mail: lesha_lysenok@ukr.net

Submission: 12/22/2020
Revision: 2/8/2021
Accept: 3/4/2021

ABSTRACT

Electronic financial services are of key importance in the EU. However, the actual policies adopted in the field by individual member states differ from country to country. A great deal of legal acts have been adopted by the EU to encourage FinTech development, to prevent money laundering and in particular to lay down secure procedures of personal identification. However, measures applied by individual member states frequently differ. The purpose of this article is to focuses on actual legal instruments used by EU financial institutions and FinTech agencies in the digital environment for client identification and on major problems faced by FinTech companies rendering modern financial services. Financial institutions and FinTech agencies often face the problem of client identification which is of key importance in the field. The complex legal regulation of the field has been extended to include such concepts as customer due diligence, simplified customer due diligence,

ISSN: 2236-269X
DOI: 10.14807/ijmp.v12i3.1532

enhanced customer due diligence and customer identification in physical absence. Each of the ways of identification differs in the scope of collected personal data, methods of data collection, legal regulation and the use of technological instruments.

Keywords: Prevention of Money Laundering; Customer Identification; Customer Due Diligence; Simplified Customer Due Diligence Measures; Enhanced Customer Due Diligence; Electronic Signature

1. INTRODUCTION

As the market of payment instruments is growing, the choice of a suitable on-line service scheme becomes an important issue for new players in the market. Newly emerged FinTech businesses have already updated their business models. So far, Lithuania has been positioned as a state having an innovative FinTech sector and encouraging FinTech market players to deliver their services on the Internet. Distance customer identification is crucial here. Therefore, we face a constantly growing need to legally regulate the process of distance customer identification so that not to violate principles of technological neutrality and functional equivalence.

Customer identification has become a key element of interior control of financial institutions since suitable customer identification is essential for financial institutions to avoid possible misuse and fraud by the client. However, the key and the most important reason for strict customer identification procedures is prevention of possible money laundering and financing of terrorism stipulated in legal acts of the EU.

Strict standards of the customer identification procedure stem from the directive 91/308/EEC of 1991 *on prevention of the use of the financial system for the purpose of money laundering* (Council Directive, 1991), being the first instrument to bind member states to ban anonymous accounts and anonymous payment cards in their financial and credit institutions. Thus, financial institutions in all EU member states have no right to service anonymous accounts.

A few years earlier, in 1989, Financial Action Task Force was launched with the key goal to combat shadow economy and monitor new trends and technologies. To achieve the goal, FATF adopted 40 recommendations on combating money laundering (Fatf Recommendations, 2012). In 1996, FATF recommendations were revised in view of the use of rapidly developing IT technologies for the purpose of money laundering and of the growing

ISSN: 2236-269X
DOI: 10.14807/ijmp.v12i3.1532

number of electronic payment services companies, most of which were not even registered as ordinary financial institutions. 130 countries approved and adopted the recommendations, which became the key standard in anti-money laundering policies.

The aforementioned FATF recommendations were transposed to the first EU anti-money laundering directive. In particular, the tenth FAFT recommendation "*Financial institutions should be prohibited from keeping anonymous accounts or accounts in obviously fictitious names. Financial institutions should be required to undertake customer due diligence (CDD) measures.....*" makes a serious challenge for financial institutions and the new FinTech sector – offering up-to-date financial services by means of digital aids and on-line client identification procedures.[1] In 2018, the FATF plenary meeting emphasized the importance of the FinTech sector and the need to encourage use of new technologies in the financial sector and increase efficiency of money laundering prevention.(Outcomes Fatf Plenary, 2018)

Importance of the FinTech sector and development of innovative tools of distance verification of customer identity have also been emphasized by European Banking Authority in their official opinion: "there are innovative solutions that often involve non-face-to-face verification of customers' identity on the basis of traditional identity documents (e.g. a passport, a driving licence or a national identity card) through various portable devices such as smartphones" (Opinion of 23 JANUARY, 2018).

2. RESEARCH PROBLEM

The new challenge closely associates with differences between data processing in physical and digital environments. In a physical environment, a personal identification document is enough to verify one's identity. Personal identity documents issued by the state form legal identity of the holder. The most important legally acknowledged documents verifying one's identity typically in a physical environment include an ID card and a passport.

The latter are granted by authorized national institutions and constitute the only legally valid identity verification instrument in most member states of the EU (Prado). Financial institutions in the EU are imposed a duty to duly verify customer identity in a physical

[1] For example, amendments in Lithuania's legislation made in 2013 allow financial institutions deal with the customer (including non-citizens) without their physical presence on submission of a qualified certificate.

ISSN: 2236-269X
DOI: 10.14807/ijmp.v12i3.1532

environment (Directive, 2018/843) since[2] physical identity verification in presence of the customer is deemed more reliable than that done in their absence. The same approach is typical in most EU member states including Lithuania. Controlling agencies carefully monitor identity verification processes and personal data collected by financial institutions.

However, the argument that customer identity verification is more reliable in a physical environment has no serious grounds and has become obsolete. As international migration has become common place, nation states are facing the need to introduce reliable tools of personal identity verification and establish a reliable link between the holder and the document at the moment of crossing the border, leading the EU to the adoption of a decision on the use of biometric data as a new standard of personal identification, Minimum security standards for passports were introduced by a Resolution of the representatives of the Governments of the Member States, meeting within the Council, on 17 October 2000.

It is now appropriate to upgrade this Resolution by a Community measure in order to achieve enhanced harmonised security standards for passports and travel documents to protect against falsification. At the same time biometric identifiers should be integrated in the passport or travel document in order to establish a reliable link between the genuine holder and the document" (Council Regulation No 2252/2004). Biometric data may be collected and used only within the limited scope of subjects.

Also, the data may be collected and processed only by a single institution within the state "In order to ensure that the information referred to is not made available to more persons than necessary, it is also essential that each Member State should designate not more than one body having responsibility for producing passports and travel documents, with Member States remaining free to change the body, if need be. For security reasons, each Member State should communicate the name of the competent body to the Commission and the other Member States (Council Regulation No 2252/2004).

Ambitions to use biometric data recorded in personal identity documents for the purpose of rendering financial services were blocked by the ECJ decision of 2013 "The regulation not providing for any other form or method of storing those fingerprints, it cannot in and of itself, as is pointed out by recital 5 of Regulation No 444/2009, be interpreted as providing a legal basis for the centralised storage of data collected thereunder or for the use of

[2] Identity verification in the digital environment cannot grant the same rights to financial services as in the case of physical presence. Available amounts and turnovers are limited here.

ISSN: 2236-269X
DOI: 10.14807/ijmp.v12i3.1532

such data for purposes other than that of preventing illegal entry into the European Union" (Judgment of the Court, 2013).

It has to be acknowledged that technical specifications of personal identity instruments, such as standards and functioning of biometric data storage, is a sensitive issue subject to usage limitations. Efficiency of the EU border protection would be significantly lower if technical specifications of personal identity instruments became public and available for the purpose of commercial interaction: "This Regulation should lay down only such specifications that are not secret. These specifications need to be supplemented by specifications which may remain secret in order to prevent the risk of counterfeiting and falsifications" (Council Regulation No 2252/2004).

The aforementioned arguments are enough to prevent EU financial institutions from the use of biometric data recorded in personal identity documents for the purpose of identity verification in a physical environment.

There are no objective reasons to argue that physical identity verification by collecting "relevant copies of identification and verification data" (Directive 2018/843) is more reliable than the one made by way of electronic means since (Law of the Republic of Lithuania on Prevention of Money Laundering and Terrorist Financing).

1) the staff of financial institutions are not experts in forensic document examination despite the fact that legal acts stipulate the obligation " to assess appearance of the document checking in particular if the photo, individual pages or included records have not been changed or corrected". This is an absolutely declarative norm practically impossible to enforce. The used legal technique is inappropriate while the standard *checking in particular* is vague. The required performance takes special knowledge and expertise possessed by forensic experts and not by front liners of financial institutions.

2) Employees of financial institutions are technically unable to authoritatively "assess if the customer (customer's representative) acting as a natural person has submitted a valid document to the financial institution or any other authorised individual and identify if the submitted document contains an authentic photo of the customer". Comparison of the physical appearance with the photo in the document is not absolutely reliable as individual people have different face recognition skills and abilities. Scientific research reveals that such skills are very individual and divergent: "Understanding the nature of individual differences in ability to perceive and recognise face identity is of importance

ISSN: 2236-269X
DOI: 10.14807/ijmp.v12i3.1532

in real-life contexts ranging from eye-witnessing to passport control..../ different aspects of face-perception abilities to associate with more general tasks in quite specific and differentiated ways" (Mccaffer, 2018). EU financial institutions frequently deal with clients of Asian origin and face recognition becomes a serious challenge to employees of financial institutions responsible for customer identity verification. Researchers in image recognition argue that "by assembling a large data set of labelled images and experimenting with different neural network architectures, we have achieved a remarkable accuracy 75.03%, almost twice as high as the human average accuracy" (Yu Wang, 2016) In other words, a human being is unable to recognize faces with 100%accuracy, which is only a declarative norm practically impossible to follow without a technical biometric data analysis.

3) EU legal acts lay down a requirement for financial institutions to collect necessary documents, data and information directly from national data systems and registers (Directive 2018/843); however, this is enough only to verify document authenticity and not the dependence to the holder whose identity is subject to verification.

The purpose of this article is to focuses on actual legal instruments used by EU financial institutions and FinTech agencies in the digital environment for client identification and on major problems faced by FinTech companies rendering modern financial services. Financial institutions and FinTech agencies often face the problem of client identification which is of key importance in the field

3. METHODOLOGY

Methodologically, this research focuses on the regulation of prevention of money laundering in the EU and Lithuania, and also on the understanding of client identification. The authors use qualitative research methods, such as the method of textual analysis and the analysis of case law.

4. RESULTS

In 2005 the EU adopted a directive (Directive 2005/60/EC) on the prevention of the use of the financial system for the purpose of money laundering and terrorist financing including newly introduced identity verification concepts of due diligence measures and simplified customer due diligence measures. The concept of simplified customer due diligence measures entails simplified customer identity verification standards. Strict identity verification

ISSN: 2236-269X
DOI: 10.14807/ijmp.v12i3.1532

procedures can be omitted where the risk of money laundering is low.

The same directive also includes an option of conditional anonymity[3] applicable in cases of limited sums, payments and e-transactions.

Until 2013, Lithuania's financial institutions had no legal opportunities to verify customer identity on the basis of their electronic ID, although qualified electronic signatures were already available at several agencies.[4] In 2013, Lithuania's government adopted decision (Resolution NO 942, 2008) to amend the existing identity verification procedures. The decision allowed identity verification without physical presence of the customer.

"Financial institutions and other economic operators shall be entitled to verify identity of their customer holding Lithuanian citizenship without the physical presence of the latter, i.e. by way of distance verification on the basis of a qualified electronic signature solely in cases where the qualified certificate was issued on the holder's identity verification in their physical presence" (Resolution no 942, 2008).

The right to use qualified certificates was granted only for Lithuanian citizens while certificates of non-Lithuanian citizens could not be used even if they were issued in the EU. Although Lithuania was already taking part in EU's single identification project STORK[5], the essence of which was the opportunity for EU citizens to use their electronic identity all over the EU, financial services were left out as an exception.

Although the aforementioned directive of 2015 does not directly refer to distance identity verification or electronic signature, member states were given an opportunity to choose to allow customer identity verification on the basis of documents, data or information collected from a reliable independent source (Directive 2005/60/EC).

It was the occasion when the a qualified electronic signature was first acknowledged equivalent to paper documents used by financial institutions for identity verification before entering into business relationships. Not all financial institutions opted for the opportunity, but the directive was of particular importance to electronic financial agencies lacking a developed physical customer service network.

3 Conditional of anonymity means a possibility to refuse certain requirements of identity verification where limited sums are in question. However, when the set limit is exceeded, financial services immediately become subject to due diligence measures.

4 Types and technical issues of the electronic signature will not be discussed here as research focuses only on its application in the financial sector.

5 The aim of the STORK project was 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.

ISSN: 2236-269X
DOI: 10.14807/ijmp.v12i3.1532

Amendments to the directive made in 2018 (Directive 2018/843) stipulated explicitly that a qualified electronic signature is a suitable means of identity verification applicable in all member states independently on the customer's citizenship. The amendments additionally tightened the use of conditional anonymity in e-commerce transactions leaving member states an opportunity to choose independently whether to allow anonymous prepaid cards or not: „Member States may decide not to accept on their territory payments carried out by using anonymous prepaid cards.“, Lithuania chose to allow the use of such cards since 2020-07-10. (Law of the Republic of Lithuania on Prevention of Money Laundering and Terrorist Financing).

Much more important amendments of the directive were made on distance identity verification: „identifying the customer and verifying the customer’s identity on the basis of documents, data or information obtained from a reliable and independent source, including, where available, electronic identification means, relevant trust services as set out in Regulation (EU) No 910/2014 of the European Parliament and of the Council or any other secure, remote or electronic identification process regulated, recognised, approved or accepted by the relevant national authorities;“. Apart from specific measures to enforce the electronic signature, member states are also allowed to independently choose, regulate, acknowledge and approve processes of electronic identification.

The amendments of the directive have been transposed into Lithuania's legal system. (Picture 1). Lithuania's legal acts clearly stipulate the procedure of customer or beneficiary identification without the physical presence of the latter. The aforementioned limitation on citizenship was revoked to allow identity verification of non-Lithuanian citizens by means of electronic identity instruments issued in the EU and compliant with high or substantial electronic identification assurance schemes or by means of qualified electronic signature certificates compliant with requirements set in Regulation (EU) Nr. 910/2014 (Regulation (EU) NO 910/2014). Lithuania's financial institutions may offer their services to customers holding qualified certificates issued in EU member states or certificates included in the EU Trusted List of Trust Service Providers (Trusted List Browser).

Another important aspect is that Lithuania's regulation of the use of distance identity verification still retains a redundant requirement imposing upon a financial institution an obligation to make sure the electronic signature was issued on identification of the customer in their physical presence: "customer's identity was established in customer's physical presence at the moment of issuance of an electronic identity instrument, compliant with high or substantial

ISSN: 2236-269X
DOI: 10.14807/ijmp.v12i3.1532

electronic identification assurance schemes, or before issuing a qualified electronic signature certificate".

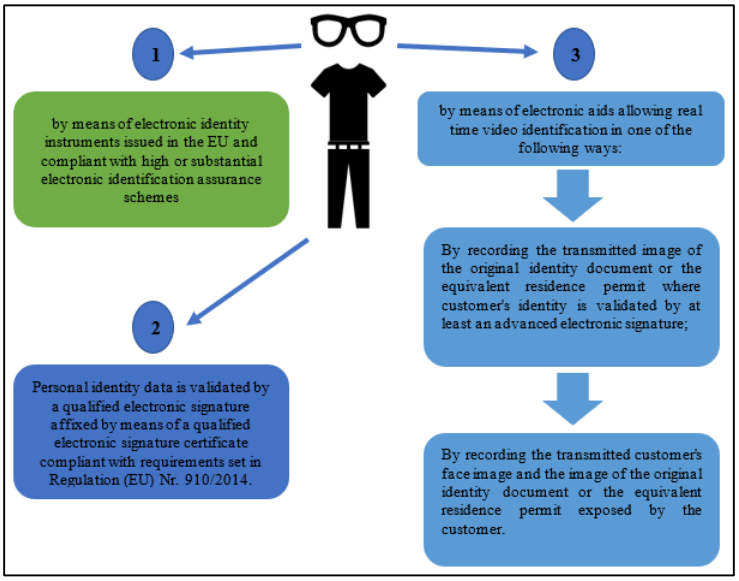

Figure 1: Requirements for customer or beneficiary identification where the identity is established without physical presence of the customer or beneficiary
Source: compiled by the authors

The very fact of such requirement can make one wonder if Lithuania's legislature calls into question proper implementation of Regulation (EU) No 910/2014 in EU member states, which is about electronic identification aids with high security assurance and the qualified electronic signature issued as an equivalent to a physical document with an equivalent legal effect.

Regulation (EU) No 910/2014 states that the security assurance level should describe the level of reliability of the electronic identification instrument in identity verification and ensure that an individual claiming to have a certain identity is actually the person the identity in question is ascribed to. Minimum technical requirements, standards and procedures applicable to ensure low, substantial or high security level should also be paid attention to. According to the Regulation, a high security level is essential in issuance of qualified electronic identification certificates.

The set requirements have to be technologically neutral and possible to meet by means of various technologies. (Regulation (EU) NO 910/2014). If a qualified electronic signature has been issued by a body included into EU Trusted List of Trust Service Providers, it may be presumed that the issuer is of "high security level essential in issuance of qualified electronic identification certificates" and has unequivocally verified person's identity before granting a qualified electronic signature.

ISSN: 2236-269X
DOI: 10.14807/ijmp.v12i3.1532

Financial institutions are bound by the valid regulation and have to rely on data by EU Trusted List of Trust Service Providers whereas Lithuania's legal provisions are in conflict with the position of the EU Commission stating that "trusted Lists are therefore essential in ensuring certainty and building trust among market operators as they indicate the status of the service provider and of the service at the moment of supervision, while aiming at fostering interoperability of qualified trust services by facilitating the validation of, among others, eSignatures and eSeals" (Shaping Europe's Digital Future).

So far, Lithuania has retained the requirement for financial institutions to make certain and ensure that the used identification instrument is compliant with the aforementioned requirement, that is the customers identity was verified in their physical presence before granting a qualified electronic signature certificate. At the same time, it has to be noted that the responsibility for compliance with requirements set for customer or beneficiary identification when the identity is verified without their physical presence lies on the financial institution. Such requirement leads to certain problems:

1) Lithuania's financial institutions cannot automatically accept EU issued qualified certificates.

2) On receipt of such certificates, the financial institution has an obligation to inquire data about the identity verification procedures from the certificate issuer. Also, in customer or beneficiary identification by means of a qualified certificate and without physical presence of the customer, financial institutions verifying customer or beneficiary identification are bound to use additional data, documents or information allowing verification of the authenticity of the customer's identity.

EU citizens are free to use qualified certificates, sign contracts, enjoy public e-services and access sensitive health data within the entire EU, but they are actually precluded from the use of financial services in Lithuania.

In future, customers of financial institutions will be allowed to use a simpler way of distance identity verification by means of electronic tools allowing real time video identification (Picture 1). However, such way entails a problem of matching the transmitted video image to the image contained in the document. When matching is done visually, we face the problem of reliability, which has already been discussed in the article. Most of EU member

ISSN: 2236-269X
DOI: 10.14807/ijmp.v12i3.1532

states rely upon distance identity verification techniques based on image transmission.[6]

In customer or beneficiary identification without physical presence of the customer, financial institutions are bound not only to ascertain and verify identity of the customer or beneficiary, but to refer to additional data, documents or information necessary for the purpose of customer or beneficiary identification and allowing verification of the authenticity of the customer's identity and find out if there are grounds to apply enhanced identity verification as well.

The requirement to use additional data applies in all cases including those where a secure electronic signature is used. Even when it is known that a person's physical presence during their identity verification cannot grant absolute accuracy of identification, but there is no additional requirement of mandatory verification of the beneficiary's identity, client identification is presumed to have been properly verified in cases of inter-institutional money transfers and there is no obligation for the receiving institution to additionally verify beneficiary's identity. Moreover, the grounds for the receiving institution to claim customer's personal data from the transferrer remain uncertain.

When money is transferred to your account from another financial institution, your personal identity data, verified with due diligence by your account provider, are not normally passed to the transferring financial institution. However, if the customer opts for distance identity verification, any operations will be carried out only on approval of the recipient's identity, which can hardly be done without violation of principles of personal data protection.

A uniform practice in the field is absent – financial institutions rely upon individual solutions of distance customer identification.

Lithuania's supervisory bodies are reluctant to go deeper into the problem and legal grounds to claim recipient data without the consent of the recipient are still absent. For example, if a fixed sum is transferred within the eurozone by means of EU payment systems, the data necessary for the transaction include an IBAN number and the purpose of payment whereas the name and the surname of the recipient are not mandatory. Where the transfer is

[6] Source: adapted from Report on existing remote on-boarding solutions in the banking sector Assessment of risks and associated mitigating controls, including interoperability of the remote solutions. European Commission

Directorate-General for Financial Stability, Financial Services and Capital Markets Union. December 2019.

ISSN: 2236-269X
DOI: 10.14807/ijmp.v12i3.1532

between EU financial institutions, the sum will be transferred to the recipient's account on submission of any name. Thus, the most important identifier in money transfer within the eurozone is the IBAN number.

Practical implementation of the requirement to identify the beneficiary becomes rather complex as it is uncertain which body has to supply the data. The receiving financial institution cannot disclose personal data of the IBAN holder on request by the sending institution. Even when the sending financial institution requests the sender to submit data on the beneficiary, there are no legal grounds for the sending institution to disclose personal data without their customer's consent. Financial institutions find themselves in a situation where the redundant requirements become impossible to meet and the provider of financial services is actually forced to violate legal regulations and risk facing a penalty.

Although the new directive of 2018 (Directive, 2018/843) granted wider opportunities to use distance identity verification, safe electronic recognition tools of the same legal force and effect, a qualified electronic signature and a possibility to choose means of real time video identification, financial institutions chose to implement different technical solutions (European Commission Directorate-General For Financial Stability, Financial Services and Capital Markets Union, 3 (2019) (Table 1).

Another strict requirement valid in Lithuania concerns cases of distance identification of residents of third countries rated by European Commission as high risk countries (European Commission, 2019). Where the customer is resident of any of the aforementioned 23 countries, Lithuania's financial institutions are instructed to mandatory ensure that "the first payment by the customer be made through an account in the customer’s name with a credit institution registered in an EU member state or a third country stipulating requirements equivalent to parallel requirements laid down in the present Act and monitored by competent supervisory bodies"

It has to be noted that Directive (EU) 2018/843 provides that „Member States may require obliged entities to ensure, where applicable, that the first payment be carried out through an account in the customer’s name with a credit institution subject to customer due diligence standards that are not less robust than those laid down in this Directive”.

Words "ensure, where applicable" are of key importance here. In other words, such payment may be requested if necessary, in case of a specific customer, but not in all cases. Why Lithuania chose to impose the requirement universally remains uncertain. Also, the directive

ISSN: 2236-269X
DOI: 10.14807/ijmp.v12i3.1532

refers to credit institutions and not to financial in general, meaning that customers of electronic money institutions are even unable to make such payment until they open a bank account in one of EU member states. For example, a customer in Tunisia is unlikely to have an account in a European bank and there is still no approved list of third countries complying with EU standards of anti-money laundering.

It is unclear why Lithuania's legislator has chosen such model. It actually hinders development of modern FinTech services (as registration in Lithuania entails applicability of Lithuania's legal regulation).

Why physical identity verification is deemed more reliable than online also remains in question. Why is additional data needed for distance identification by a secure electronic signature, when the electronic certificate already contains all necessary personal data? Why is video identification subject to additional requirements although the identity document may be clearly exposed here and modern technologies allow comparison of unique biometric data, which is impossible in the physical environment where identification is deemed more reliable?

Table 1: The main obstacles for involvement of respondents in eLearning

NETHERLANDS	Video identification or equivalent technique is associated to automatic transfer data from the id document to the relevant (liveness check)
UNITED KINGDOM	Video Identification is used in association with electronic verification Remote onboarding is used primarily by newer, challenger banks who are online only and do not have branch network.
BELGIUM	Use of video identification is possible since Customer ID should be verified against one or more supporting documents or reliable and independent sources of information which enable obliged entities to confirm this data
LUXEMBOURG	Video identification permitting the delivery by Luxtrust of eIDAS-qualified electronic signature services
FRANCE	Video identification + biometry is used (Currently no regulation governs video identification. A regulation on remote onboarding which will validate an eIDAS scheme is being prepared. Both substantial and high e-ID will be in scope of the regulation. Solutions are based on picture comparisons between the picture contained in an official identity paper (passport or id card) and a selfie.)
LIECHTENSTEIN	Video identification
ITALY	Video identification and biometrics or other technology solutions
PORTUGAL	Use of video conference (e.g. Caixa Geral de Depositos) in addition with biometrics (Banco BNI Europa) For these use cases, the legislation requires financial institutions to have a person, in real time, validating the client’s identity.
SPAIN	Video identification systems is used. In some cases, in addition with electronic signature. Regulation is in place for both attended and unattended video identification. Widely used for mobile on-boarding by most banks and in some cases also for web-based (BBVA, Santander, OpenBank, ImaginBank, Self Bank, Evo Banco and Bankia)
GERMANY	Pursuant to BaFin Circular 3/2017 Video-Identification is a recognized form of identification procedure in accordance with the AML Act in Germany
ESTONIA	Video identification (can be completed with biometrics)
LATVIA	Video identification (acquisition of data accrediting the identity of a natural person from a credit institution or payment institution)
POLAND	Use of Video-identification with or without biometry
SLOVAKIA	Video call identification (via special application of the bank)

ISSN: 2236-269X
DOI: 10.14807/ijmp.v12i3.1532

AUSTRIA	Identification through video-chat has been approved by the Austrian Financial Market Authority (FMA) on 3 January 2017.
ROMANIA	Video identification.
HUNGARY	Real time video identification via comparison of the ID photo with the of customers. Used by OTP Bank, Gránit Bank, Takarék Kereskedelmi Bank, Cofidis Bank, MKB Bank.
SLOVENIA	Video identification + Identity card check is permitted to on board customer for account opening.
MALTA	Video Identification: The (prospective) customer's identity is verified during a video conference call

Source: adapted from Report on existing remote on-boarding solutions in the banking sector

The number of EU countries where financial institutions introduce modern identity verification aids is growing. Legal environment has become favourable to FinTech development. However, legal regulation in Lithuania is still limiting development of the service. Lithuania has been positioning itself as a FinTech leader in the UE (Lithuania's Impressive Fintech Growth Extends, 2020) emphasizing clarity, transparency and rapidness of licensing essential for FinTech businesses. However, the disproportionate legal regulation of the process of identity verification in the electronic environment may trigger problems forcing FinTech companies to move their business outside Lithuania.

FinTech business is not limited by national boundaries and trade their services in the electronic environment to customers from all over the EU and even outside the EU. FinTech companies working in the sphere of e-money and e-payment may be drawn as an example (Picture 2). If they had started in Lithuania, they would not be able to offer their services outside Lithuania as successfully as they are doing now from other countries. The success directly depends on legal regulation of identity verification, application of additional requirements and newly introduced practices.

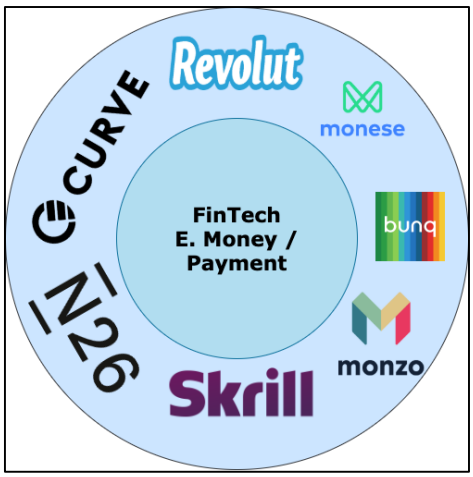

Figure 2 - FinTech companies using video identification as a means of identity verification

Compiled by the authors

5. CONCLUSIONS

ISSN: 2236-269X
DOI: 10.14807/ijmp.v12i3.1532

Lithuania has been positioned as a state with a FinTech-friendly environment. However, its national legal acts and practices of supervisory bodies impose disproportionate regulation of identity verification procedures in the electronic environment. The physical process of identity verification is given a priority as more reliable than distance identification – a conclusion arrived at having analysed requirements set upon the identity verification procedure.

The distance identity verification procedure based on a secure electronic signature issued in the EU is being hampered by an excessive requirement to make sure the electronic signature was issued on identification of the customer in their physical presence. It seems that Lithuania's legislature calls into question monitoring and performance of secure qualified electronic signature issuers even where the issuer complies with requirements stipulated by the European Commission.

In case of video identification, customers face additional requirements to disclose personal data of third-party beneficiaries along with submission of their own personal data, which is already present in the submitted documents, although the requirement is absent in case of physical customer identification.

Directive (EU) 2018/843 provides the right of nation states to use their own discretion in deciding on the applicability of enhanced identity verification and the requirement to make the first payment through an account at a bank registered in the EU. However, the provision "may require obliged entities to ensure, where applicable" has been transposed to Lithuania's legislature as the requirement" to ensure that the first payment by the customer be made through an account in the customer’s name with a credit institution registered in an EU member state or a third country stipulating requirements equivalent to parallel requirements laid down in the present Act and monitored by competent supervisory bodies.

At the moment of writing this article, there was still no approved list of third countries complying with EU standards of anti-money laundering.

REFERENCES

Biometric passport Fingerprints Regulation (EC) No 2252/2004 Article 1(2)

Cardoso, W.; Azzolini, W.; Bertosse, J.F.; Bassi, E.; Ponciano, E.S.(2017). Digital Manufacturing, Industry 4.0, Clould Computing and Thing Internet: Brazilian Contextualization And Reality. **Independent Journal of Management & Production,** 8(2), 459-473. **DOI:** 10.14807/ijmp.v8i2.572.

ISSN: 2236-269X
DOI: 10.14807/ijmp.v12i3.1532

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

Council Regulation (EC) No 2252/2004 Of 13 December 2004 On Standards for Security Features and Biometrics in Passports and Travel Documents Issued by Member States THE COUNCIL OF THE EUROPEAN UNION.

Directive (EU) 2018/843 of the European Parliament and of the Council of 30 May 2018 amending Directive (EU) 2015/849 On the prevention of the use of the financial system for the purposes of money laundering or terrorist financing, and amending Directives 2009/138/EC and 2013/36/EU (Text with EEA relevance) PE/72/2017/REV/1.

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.

Directorate-General For Financial Stability, Financial Services and Capital Markets Union. December 2019.

European Commission adopts new list of third countries with weak anti-money laundering and terrorist financing regimes. Today, the Commission has adopted its new list of 23 third countries with strategic deficiencies in their anti-money laundering and counter-terrorist financing frameworks. Avaible: https://ec.europa.eu/commission/presscorner/detail/en/IP_19_781.

FATF Recommendations 2012 - adopted on 16 February 2012 and updated regularly since.

Ghotbifar, F.; Marjani, M.; Ramazani, A. (2017). Identifying and Assessing the Factors Affecting Skill Gap in Digital Marketing in Communication Industry Companies. **Independent Journal of Management & Production,** 8(1), 1-14. DOI: 10.14807/ijmp.v8i1.507.

Gurgu, E., Gurgu, I.A., & Tonis, R.B.M. (2020). Neuromarketing for a Better Understanding of Consumer Needs and Emotions. **Independent Journal Of Management & Production,** 11(1), 208-235. DOI: 10.14807/ijmp.v11i1.993.

Judgment of the Court (Fourth Chamber) 17 October 2013 (*1). Reference for a preliminary ruling Area of freedom, security and justice.

Laurinaitis, M., Stitilis, D., Rotomskis, I., Azizov, O., & Marchuk, N. (2020). Limitations of the Concept of Permanent Establishment and E-commerce. **Independent Journal of Management & Production,** 11(9), 2308-2324. DOI: http://dx.doi.org/10.14807/ijmp.v11i9.1429.

Law Amending Article 168 of the Code of Criminal Procedure of the Republic of Lithuania. Document No. VIII-275. Amendments no. XIII-2584, 03/12/2019, published in TAR on 19/12/2019.

Law of the Republic of Lithuania on Prevention of Money Laundering and Terrorist Financing no. VIII-275 2, 4, 5, 7, 8, 9, 10, 11, 12, 13, 14, 15, 17, 19, 20, 21, 22, 23, 24, 25, 26, 27, 28, 29 , 48, 49, 51 and the Law amending and supplementing the Annex with Articles 71, 141, 251, 252. (2019). December 3 No. XIII-2584, Vilnius.

Lithuania's Impressive Fintech Growth Extends (2020). Available: https://investlithuania.com/news/lithuanias-impressive-fintech-growth-extends-into-2020/. Access: 11 September 2020.

ISSN: 2236-269X
DOI: 10.14807/ijmp.v12i3.1532

Mccaffery, J. M., Robertson, D. J., & Young, A. W. (2018). Individual differences in face identity processing. **Cogn. Research,** 3, 21. https://doi.org/10.1186/s41235-018-0112-9.

Opinion of 23 January 2018 on the use of innovative solutions by credit and financial institutions in the customer due diligence process. European Banking Authority.

Prado - Public Register of Authentic travel and identity Documents Online. European Parliament. European Commission.

Puraite, A., Zuzeviciute, V., Bereikiene, D., Skrypko, T., & Shmorgun, L. (2020). Algorithmic Governance in Public Sector: Is Digitization a Key to Effective Management. **Independent Journal of Management & Production,** 11(9), 2149-2170. DOI: http://dx.doi.org/10.14807/ijmp.v11i9.1400.

Regulation (EU) No 910/2014 of the European Parliament and of the Council of 23 July 2014 on electronic identification and trust services for electronic transactions in the internal market and repealing Directive 1999/93/EC.

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. (has been revoked).

Shaping Europe's Digital Future. Policy. EU Trusted Lists. European Commission. https://ec.europa.eu/digital-single-market/en/eu-trusted-lists-trust-service-providers

Stitilis, D., Rotomskis, I., Laurinaitis, M., Nadvynychnyy, S., & Khorunzhak, N. (2020). National Cybersecurity Strategies: Management, Unification and Assessment. **Independent Journal of Management & Production,** 11(9), 2341-2354. DOI: http://dx.doi.org/10.14807/ijmp.v11i9.1431.

The Financial Action Task Force (2018). Outcomes FATF Plenary, 17-19 October 2018.

Trusted List Browser. Tool to browse the national eIDAS Trusted Lists and the EU List of eIDAS Trusted Lists (LOTL). Avaible: https://webgate.ec.europa.eu/tl-browser/#/. Access: 15 September 2020.

Validity Legal basis Procedure for adopting. Articles 7 and 8 of the Charter of Fundamental Rights of the European Union Right to respect for private life Right to the protection of personal data Proportionality.

Viltard, L.A. (2016). Unlimited, Blurred limits in a borderless world. **Independent Journal of Management & Production,** 7(2), 380-412. DOI: dx.doi.org/10.14807/ijmp.v7i2.417.

Yu Wang, Haofu Liao, Yang Feng, Xiangyang Xu, & Jiebo Luo (2016). **Do They All Look the Same? Deciphering Chinese, Japanese and Koreans by Fine-Grained Deep Learning.** Department of Computer Science. University of Rochester, NY, USA. arXiv:1610.01854v2 [cs.CV]. 23 Oct 2016.