Implementing Innovative Customer Due Diligence: Proposal for Universal Model

Dr. Victor DOSTOV, greygato@gmail.com Saint-Petersburg State University, 199034, 7-9 Universitetskaya Emb., St Petersburg, Russia; Russian Electronic Money and Remittance Association, 107078, 5/2 Orlikov per., Moscow, Russia, https://orcid.org/0000-0003-4518-2883

Dr. Pavel SHUST, paul.shoust@gmail.com Saint-Petersburg State University, 199034, 7-9 Universitetskaya Emb., St Petersburg, Russia; Russian Electronic Money and Remittance Association, 107078, 5/2 Orlikov per., Moscow, Russia, shoust@npaed.ru, https://orcid.org/0000-0002-2276-7523

Abstract

Purpose – The purpose of this paper is to present the identification-verification-confirmation of identity (IVCid) model that can be used to retroactively analyze the existing customer identification programs and devise new ones that can be used in face-to-face or non-face-to-face environment.

Design/methodology/approach – This paper outlines the main elements of the customer due diligence (CDD) process and identifies those which may present a barrier to the customers. It then outlines the IVCid model. The model is used to analyze existing CDD approaches in physical presence, using reliable databases, biometrics and electronic signatures.

Findings – The IVCid model suggests that any customer identification program contains three elements: identification (collection of information), verification (checking the veracity of information) and confirmation of identity (linking the information to the individual). The accuracy of this model is confirmed by the analysis of the existing CDD procedures in some countries.

Research limitations/implications – This paper looks at a limited number of practical cases of CDD implementation. Further research might be needed to assess the strengths and weaknesses of biometric-based or e-signature-based solutions. Research might be needed to establish links between the IVCid model and financial inclusion.

Practical implications – The IVCid model allows for“modular” approach for the CDD procedures. It also underlines some risks associated with current CDD models.

Social implications – The IVCid model can be used to devise the CDD procedures that more effectively contribute to financial inclusion.

Originality/value – This paper proposes the first universal model for the CDD procedures that works for both face-to-face and remote scenarios while also being technology- and business-neutral.

Keywords Financial inclusion, Model, Customer due diligence, Biometrics, AML/CFT, Verification of identity

Paper type Research paper

1. Introduction

Prohibition on anonymous accounts goes back to the first edition of Financial Action Task Force (FATF) Recommendations in 1990. The concept has greatly evolved since. Now, the financial institutions are expected to implement detailed customer due diligence (CDD) programs to make sure that they have an in-depth understanding of their client. Apart from providing valuable information to law enforcement agencies, if needed, the CDD also allows to assess money laundering/terrorism financing (ML/TF) risks associated with a customer. A subset of the CDD is a process customarily called Customer Identification Program (CIP) [1] in short, making sure the person is one he/she says at the onboarding stage. The CIP is a highly technical procedure and poses a challenge for the developing countries and their financial institutions, especially as they are trying to use new technologies to promote financial inclusion. In this paper, we propose the identification-verification-confirmation of identity (IVCid) model that can be used to implement new CIP procedures to individuals and assess the effectiveness of those already in place. The model is based on the FATF Recommendations and can be easily integrated in the FATF guidance.

2. Literature review

There is a relatively extensive body of literature on the anti-money laundering and combating financing of terrorism (AML/CFT) regime. The research is mainly focused on the activities of the FATF or, broadly speaking, the regime that is built around it, including FATF-focused procedures such as mutual evaluations. Interestingly, most authors underline the "fuzziness" of the current AML/CFT standards.

Duyne et al. (2018) point out the lack of conceptual clarity: "perhaps fuzzy concepts are felt to be useful, because they allow a circumvention of the sharp edges of precision. The risk-based approach is an example of this fuzziness". Turner and Bainbridge,(2018) state that "proportionality and effectiveness are real concerns predominantly for private sector end users and that they can all too easily be swept aside by high-level momentum and exaggerated fears that together trigger the next regulatory response" in the UK. Pol (2018) also points out to the gaps in mutual evaluations' metrics, citing that poor indicators of the AML/CFT policy effectiveness may "inadvertently distract governments from higher-order crime and terrorist, prevention objectives". Demetis and Angell (2007) are concerned with the fuzziness of the concept of the risk-based approach (RBA), which makes financial institutions "nervous whether their own perception of risk will match regulatory expectations".

Overview of the related literature suggests that the current global AML/CFT requirements are too vague (and became more so with the introduction of the RBA). Apart from providing more flexibility, RBA also leads to confusion and anxiety among regulators and financial institutions about the FATF or FATF-style regional bodies (FSRB) mutual evaluations.

The academic literature has limited coverage of the CDD requirements and mechanisms. However, there are some notable exemptions. For example, Mugarura (2014) discusses CDD as a general requirement of the AML/CFT regulation and its impact on banking business. De Koker (2006) explores the relationship between the CDD measures and financial exclusion. He also provides an extensive overview of the CDD and know-your-customer (KYC) concepts and traces their development across a number of jurisdictions and standard-setting bodies. De Koker also identifies the risks of the overly cautious CDD approach that can push honest customer away from the financial sector. Similarly, Gill and Taylor present the findings from the survey of the UK financial companies on their perception of the CDD requirements. The results confirm the strain the disproportionate CDD requirements may put on a business. In total, 58.2 per cent of respondents agreed that CDD requirements can alienate new potential clients; the smaller institutions also reported higher costs of the CDD compliance (Gill and Taylor, 2004). In his 1998 paper, Mulligan (1998) mentions the ambiguity of the CDD regulations and underlines the need for more clear guidelines on how to comply with them, calling for more self-regulation on behalf of banks.

International institutions also attempt to provide some technical guidance on the subject. GSM Association (GSMA) has published a number of reports on innovative approaches to the CDD that involve mobile network operators (Kipkemboi et al., 2019; Theodorou and Yongo, 2018). Alliance for Financial Inclusion's (AFI) analytical report on KYC innovations and financial inclusion and integrity sheds light on the CDD regulations and implementation experiences in some jurisdictions (Alliance for Financial Inclusion, 2019). The Inter-Governmental Action Group against Money Laundering issued the review of the CDD-related operational practices in West Africa (GIABA, 2018). Gelb provided some insights on finding the balance between the CDD requirements and the RBA in practice (Gelb, 2016). There are also specific country-focused research studies on India (Banerjee, 2016), Russia (Dostov et al., 2018) and other markets. Basel Committee on Banking Supervision has recently integrated its 2001 Guidelines on the CDD for banks (Basel Committee on Banking Supervision, 2001) in its sound management of risks related to ML and FT (Basel Committee on Banking Supervision, 2017).

But neither of these papers can be used as a systematic guidance for introducing new CDD measures. GSMA, Basel Committee or AFI papers cannot be viewed as an official guidance and are not officially endorsed by the FATF. Rather, FATF, FSRB or Bank for International Settlements guidance cite only basic requirements toward the CDD mechanisms and can be considered a sort of "explanatory annexes" to the FATF Recommendations. Even though some of them have references to actual CDD mechanisms used in countries, these references are cited as "illustration only" and are not officially "prescriptive or exhaustive."

As mentioned by De Koker (2014), the FATF approach for the identification and verification framework is insufficiently effective in achieving the ultimate goal: to make the banks know who their customers are . But simply copying other countries' successful CDD measures does not work,

as all countries and their circumstances are different. This underlines the problem that Sotande, 2018 calls the "domestication" of the FATF Recommendations. This is a self-enforcing cycle: countries are afraid of being found non-compliant with the international AML/CFT standards, but as the wording of these standards is too loose, they are more inclined to use other's solutions rather than implement something that will work for them.

Despite the lack of academic or technical guidance, the CDD procedures are at the center of the AML/CFT discussions. Unlike screening of customers, monitoring of transactions or internal risk assessment, any changes in the CDD measures directly affect the consumers' experience. As confirmed by the FATF, onboarding processes have direct implications for the financial inclusion:

> [...] rigid CDD requirements that insist on government-issued identification documents, adopted by some countries or financial institutions, have acted as barriers to these disadvantaged populations obtaining access to the formal financial system (FATF, 2017).

The importance of effective implementation of new CDD measures is also exacerbated by the need to align the AML/CFT policies with the financial technologies and the financial inclusion policies. From this point, the efficiency of the CDD procedures goes beyond the pure AML/CFT concerns and also affects financial inclusion, competition and implementation of new technologies.

Therefore, there is clearly lack of common methodology that would go beyond mere advice to "appropriately apply RBA" or make sure that the financial institution "knows its customer." This is more relevant for the jurisdictions with rule based legal systems which cannot include mere principles in their regulatory frameworks. This paper aims at filling this gap by providing a simple model for real-life CDD mechanisms that can be used by both regulators and financial institutions.

This paper is structured as follows. First, Section 3 looks at the CDD concept and discuss some of its most problematic elements. Then, Section 4 draws the IVCid model based on "modular CDD approach." Section 5 analyzes some of the existing CDD practices using the IVCid model. Finally, we discuss some policy implications and areas for further research in Section 6.

It should be noted that we focus on the CDD measures in a retail financial sector. The proposed model might need corrections to be applied to the corporate clients; although, it can be well used for the measures aimed at individuals that act on behalf of the legal entity. We do not specifically distinguish simplified due diligence (SDD), as we are more interested in procedural side of the question. However, the IVCid model can be used for the analysis and implementation of the SDD as well.

3. The scope of CDD requirements

Confusion starts with the definitions. Multiple sources use the "KYC" and "CDD" as equivalents or without proper definition. For example, Yasin seems to be using the terms interchangeably (Yasin, 2015); Mugarura writes: "the core of the global AML paradigm is customer identification also known as "Know Your Customer (KYC)," thus using KYC as

equivalent for identification (Mugarura, 2014). Smet and Mention look at the CDD "practices" as the requirement to "Know Your Customer" (Smet and Mention, 2011). According to De Koker, the CDD superseded the term "KYC" since 2003 (De Koker, 2014). FATF (FATF Recommendation 10) uses the term "customer due diligence" in international standards while also mentioning "e-KYC" or "KYC/CDD requirements" in its financial inclusion and AML/CFT Guidance (FATF, 2017). Although discussion about the correlation of these two terms may hold conceptual value, it has, in our view, limited relevance for practical purposes. We will use the term CDD as defined by the FATF.

The FATF's CDD requirements evolved from the need to "identify, on the basis of an official or other reliable identifying document and record the identity of the clients" in its first report back in 1990 to a comprehensive standard on due diligence (FATF, 1990). According to the Recommendation 10 (FATF, 2012/2019), the following CDD measures need to be taken:

- identifying the customer and verifying that customer's identity using reliable, independent source documents, data or information;
- identifying the beneficial owner and taking reasonable measures to verify the identity of the beneficial owner, such that the financial institution is satisfied that it knows who the beneficial owner is (for legal entities and arrangements, this should include financial institutions understanding the ownership and control structure of the customer);
- understanding and, as appropriate, obtaining information on the purpose and intended nature of the business relationship; and
- conducting ongoing due diligence on the business relationship and scrutiny of transactions undertaken throughout the course of that relationship to ensure that the transactions being conducted are consistent with the institution's knowledge of the customer, their business and risk profile, including, where necessary, the source of funds.

Although there is an interpretive note to Recommendation 10, it mainly focuses on the application of the RBA to the CDD measures and does not really specify the meaning of each of the CDD step (De Koker, 2014). The FATF provides only high-level guidance, leaving the jurisdictions to apply any approach they seem fit.

From the practical point of view, some elements of the CDD procedure have more effect on the customers' experience than others. For example, the FATF Recommendations require identification of beneficial ownership for not only the legal entity but the individuals as well. But in practice, mass market clients are rarely directly involved in this procedure. In its Financial Inclusion Guidance, the FATF recognizes the challenge of identifying the beneficial owners for retail customers: "in a financial inclusion context the beneficial owner will in most instances be the individual customer him/herself, or a closely related family member" (FATF, 2017). In practice, this is relevant for absolute majority of the cases. Although not considered as a best practice in the mass market segment, the financial institutions would usually just ask the customer directly if he/she has a beneficial owner and later take a chance of detecting the straw men activities

via transaction monitoring. This means that in principle, the identification of the beneficial owner does not require any additional steps from the customer and might be as efficiently performed remotely as on-site.

Generally, the same applies to the understanding of purpose and intended nature of the business relationship. The FATF Financial Inclusion Guidance allows to infer this information from the type of transaction or business relationship. Therefore, in most cases, financial institutions will not proactively ask the mass market client the question why he/ she makes this particular transaction or opens an account/e-wallet.

By definition, the ongoing scrutiny of transactions and monitoring is implemented without active involvement of the customer and therefore "invisible" to him/her.

Therefore, in a mass market, most customers' due diligence elements are conducted behind the scene, unbeknownst to the client. However, the clients, by definition, need to be actively involved in onboarding procedure that involves identifying and verifying the identity (CIP). These identification/verification procedures are rather standardized. While financial institution may have tailored approach to high-value customers or large corporate customers (e.g. the bank official may decide to perform additional background checks), the mass market customers go through the same algorithmic process.

Because identification/verification is an additional cost to the customer, they may present a barrier for financial inclusion. While there are varying approaches across the globe, in many cases, customers still need to visit the office of the financial institution or even present excessive documentation. For example, in South Asia, 100 per cent of jurisdictions have either SDD in place or exemptions from the CDD requirements; in the Middle East and North Africa, it is only 22 per cent (The World Bank Group, 2017). This means that many jurisdictions still have to implement simplified and remote due diligence requirements.

However, despite multitude of options, the regulators have difficulties choosing between them. The concerns are always the same: can this procedure be manipulated? Is this procedure in line with the level of risk? Does this conform the FATF and assessors' expectations? The FATF documents do not answer these practical questions, and often, regulators do not have capacity to answer them themselves. Unfortunately, to date, we do not have a comprehensive model of the identification/verification procedures for the AML/CFT purposes that would answer those questions in practical terms. We propose the IVCid model to fill that gap.

4. Identification-verification-confirmation of identity model

The IVCid model is based on three variables and can be used to disaggregate and analyze any existing identification/verification procedure or develop and implement a completely new one. These three elements include: identification, verification and confirmation of identity (Figure 1). We believe that, taken together, they allow for a reliable establishment of individual's identity – either for financial or any other purposes.

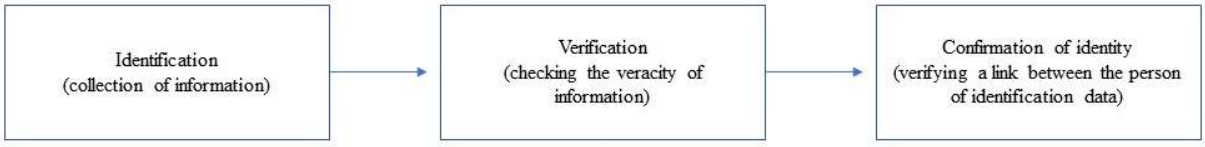

Figure 1 – Elements of IVCid model

4.1 Identification

Within the IVCid model, the identification means collection of information about the individual. Although the FATF does not lay down any list of "identity elements," i.e. data to be collected (FATF, 2013/2017), it will typically include name, date of birth and address of residence. Some jurisdictions go beyond what is required in the FATF Recommendations (The World Bank Group, 2017) and require collection of excessive information that does not necessarily help the financial institution assess and mitigate ML/TF risks and can be a source of excessive costs, but this is beyond the scope of this paper and does not affect the applicability of the IVCid model.

The information can be collected in multitude of ways and forms which will depend on whether the communication with the client is conducted in face-to-face or non-face-to-face environment (see Table 1 for a non-exhaustive list of possible options).

Table 1 – Identification proceduresTable 1

Face-to-face environment	Non face-to-face environment
Verbal (e.g. speaking with the agent or bank officer)	Verbal (i.e. providing information over a phone)
Written (e.g. by filling out the questionnaire, providing copies of documents, original documentation)	Written: via SMS, USSD, email, by filling out electronic questionnaire, by post etc.

Obviously, the data protection and data security consideration need to be taken into account when choosing the identification procedure. But generally, collection of information per se is the simplest and the cheapest element of the IVCid model. Thanks to the almost universal access to communication technologies, the information can be relayed between parties in a cheap, reliable and effective fashion.

4.2 Verification

Verification within the IVCid model means verification of the information using a reliable independent source. The goal of verification is to make sure that the person with the said characteristics (name, date of birth, etc.) actually exists.

Unlike identification, verification is a more complicated process. In compliance with the FATF Recommendations, the verification needs to be based on a reliable source of information. In a face-

to-face environment, the original documents (e.g. ID card, passport, utility bill) fit the bill. There are also "exotic" options where the referee statements (AUSTRAC, 2020) or even letters from a village representative (Alliance for Financial Inclusion, 2016) are used. In a non-face-to-face environment, the financial institution will need access to a reliable database. The exact choice of a database will depend on the jurisdiction. In some cases, this can be state-owned database, the information collected by private entities in course of their business activity (e.g. MNOs, credit bureaus, etc.) or special CDD-tailored databases.

FATF does not provide any references on what sources of information should be considered "reliable" and "independent." For example, the ID card or passport are in fact not the primary sources of information; they are merely a print-out from the issuing authority's database. Household bills are issued by the household authority with very limited responsibility for the adequacy of information. Hence, understanding of "reliability" may vary from one jurisdiction to another. According to the RBA, the financial institution shall decide on the suitability of the database itself. In rule-based jurisdictions, regulators usually specify the scope of appropriate sources of information.

In most jurisdictions, state sources are considered the most reliable. This is understandable because, after all, regulators who oversee the AML/CFT compliance of the financial institutions are part of the state and obviously trust themselves. Private sources of information are in most cases secondary to the public sources, e.g. when mobile network operators (MNOs) build up their database or landlords sign lease agreements, they use state-issued IDs that their customers present. In some cases, these sources are even tertiary, for example, credit bureaus get information from the financial institutions that got it from the state-mandated IDs. The logic suggests that the number of the intermediaries does not matter as long as they ensure the integrity and relevance of the information. In other words, if the MNO does not follow the same level of standards for identification and verification as the financial institution, its database cannot be considered reliable. To mitigate the risks or unreliability, the usage of two independent verification sources might be required, as in Australia (AUSTRAC, 2019).

It should be noted, however, that lacking universal guidance, the evaluation of reliability of databases can be speculative. For example, FATF endorses the usage of commercial databases to screen customers for politically exposed person's status but has never audited either of them. In general, their reliability is unknown and such databases are used, as there are no viable alternatives (e.g. performing Google search on every client is completely impractical).

Very much like identification, verification can be performed in both face-to-face and non-face-to-face environments.

From the procedural point of view, the remote verification is usually structured as follows:

- The information provided by the customer during identification stage is relayed to the database holder.

- The database holder compares the information with the data it holds.
- After the comparison, the database holder replies with match/no match response.

This procedure minimizes the risks of database "leakage" because the source information does not technically leave the database perimeter.

4.3 Confirmation of identity

Confirmation of identity is rarely mentioned as a separate stage of the CDD procedure and is listed as a "supplementary step" to mitigate risks of impersonation. This, in our opinion, creates confusion and misperception of risks, especially in discussions about remote CDD. Even if the verification is reliable, the regulator or the financial institution will often voice impersonation concerns. This question is valid. The verification procedure only confirms that the person exists. But it does not affirm that these particular data belong to the person. Simply speaking, the financial institution needs to make sure that the ID card presented to the bank officer is not only valid but also belongs to this particular person (Figure 2 for comparison between verification and confirmation of identity).

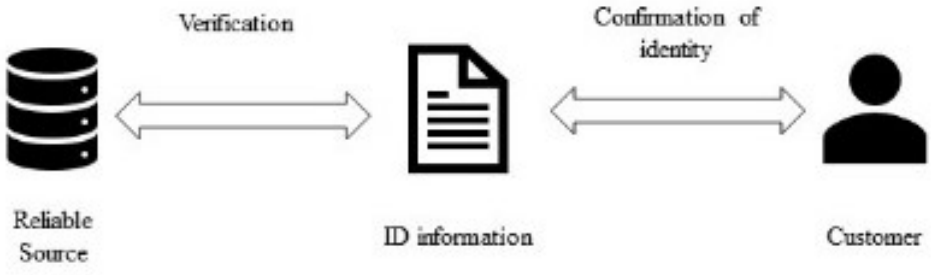

Figure 2 – Verification vs Confirmation of identity

There can be multiple ways to verify the identity of an individual. But they all seem to be based on the two-factor authentication. Two-factor authentication is currently widely used for secure access to information systems or in payments (Cimiotti and Merschen, 2014), e.g. in the European Union, the two-factor authentication (i.e. "strong customer authentication") is mandatory for most cashless transactions (Commission Delegated Regulation [EU], 2018). According to the EU's Second Payments Directive, the two-factor authentication is defined as "authentication based on the use of two or more elements categorised as knowledge (something only the user knows), possession (something only the user possesses) and inherence (something the user is) that are independent, in that the breach of one does not compromise the reliability of the others, and is designed in such a way as to protect the confidentiality of the authentication data" (Art. 4, [30]) (Directive [EU] 2015/2366 of the European Parliament and of the Council of 25 November 2015 on payment services in the internal market, amending Directives 2002/65/EC, 2009/110/EC and 2013/36/EU and Regulation [EU] No 1093/2010, and repealing Directive 2007/64/EC, 2016). While verification is aimed at establishing a link between the data provided by the client and the

reference data, strong customer authentication establishes a link between the data and the real person.

Verification of identity can be performed either remotely or in physical presence.

The three elements of the IVCid model form a reliable identification/verification procedure for the CDD purposes. As we discuss next, it can be used not only for creating new CDD approaches but also to retroactively analyze those already in use. In Section 5, we disaggregate some of the existing KYC approaches using the IVCid model.

5. Existing know-your-customer approaches

5.1 Face-to-face know-your-customer using state-issued ID

This is probably the most widespread CDD procedure in the world: the client comes to the financial institution office in person, with the state-issued ID. It is also viewed as a reference point – all other methods are qualified as "more" or "less" reliable. The IDs can have different forms, e.g. paper (as in Russia) or plastic ID card (e.g. in the USA, Azerbaijan or the Kyrgyz Republic). All IDs have the basic personal data and a photo of the holder.

Although the in-person CDD is considered conservative, it can be deconstructed using the IVCid model as well.

5.1.1 Identification. In some jurisdictions (e.g. in Kyrgyzstan [Statute on Customer Due Diligence, 2018]), the law requires that the client fills out the questionnaire that includes basic personal details (name, date of birth) by hand. In other jurisdictions, the bank officer will take the ID from the customer and enter the data into the computer system.

In essence, this is just collection of the required information from the customer. In narrow terms, the bank officer does not verify the veracity of the information but just collects it.

5.1.2 Verification. In this scenario, the ID is considered a reliable verification source. The bank officer checks the authenticity of the ID, its validity, etc. In case the person has filled out a questionnaire, it is compared to the information in the ID, and when the bank officer types the information into the computer system himself/herself, the identification and verification are typically merged (the officer verifies data as he/she copies it from the ID).

5.1.3 Confirmation of identity. Presentation of ID in person is so common and customary that we do not notice the details of this process. But yet, there is a separate confirmation of identity: the bank officer checks two factors – the possession (of the ID itself) and the inherence (the photo).

If all the stages of the IVCid model are successful, the CDD deemed successful, all other checks are either purely automatic (e.g. risk screening), based on oral testimony or inducted (e.g. purpose of the business relationship).

Apart from purely methodological value, the IVCid model also shows the potential pitfalls and deficiencies of the in-person CDD. For example, the verification stage is very much dependent on

the familiarity of the bank officer with the type of ID. This is usually not a problem when the client is a local because the bank officer has the same ID and knows how it looks. But when a client is a foreigner with exotic ID, checking the authenticity might be a problem.

Another source of risk is reliance on inherence during confirmation of identity. Essentially, the biometrics and the photo can be unreliable (e.g. when it was made a long time ago or the customer has a twin).

5.2 Remote customer due diligence using reliable databases

A few jurisdictions allow to perform the "standard" or simplified CDD using the reliable databases. For example, in Russia, customers can go through the SDD by remotely providing ID number, name and one of the "additional identifiers" such as individual tax number, social security number or medical insurance policy number (Law No 115-FZ 2001 "On countering the legalization (laundering) of criminally obtained incomes and the financing of terrorism"). This information is then verified via state databases. Quite similar approach is used in New Zealand, where Identity Verification Code of Practice allows for electronic verification using reliable electronic sources (Identity Verification Code of Practice – Explanatory Note, 2017). This is a relatively simple and cheap method both for the financial institution and the customer. But there might be some factors that can undermine the reliability of this approach. The IVCid model shows what and how can be done to mitigate these risks.

5.2.1 Identification. Collection of information can be implemented in any form. From the IVCid model's standpoint, it does not really matter if the client fills out the Web form, submits data using mobile application, tells it over the phone or even sends in an envelope over mail. The main point is to relay information from the customer to the financial institution. In practice, remote CDD usually starts with filling out the Web form.

5.2.2 Verification. The information received from the customer is then verified via a reliable database. As discussed previously, the question of reliability varies. For example, in Russia, the Tax Federal Service, Pension Fund, Ministry of Internal Affairs and Federal Compulsory Medical Insurance Fund are the only databases legally considered reliable for the SDD purposes. In Australia, credit bureaus are considered reliable. In New Zealand, Financial Market Authority allows reporting entities to choose any electronic sources taking into account accuracy, security, privacy, method of information collection, built-in confirmation of identity mechanisms and "owner" of information (Amended Identity Verification Code of Practice 2013, 2017). It should be noted that the verification of data using reliable databases shall not be qualified as "reliance on third parties" as per the FATF Recommendation 14. The third party database is used entirely for the purpose of verification of information; the third party does not perform the CDD themself; therefore, the holder of the database does not need to be a reporting entity or send original documents on request.

5.2.3 Confirmation of identity. The financial institution needs to ensure that the person is who he/she says he/she is. In this CDD scenario, this is tricky. Just asking for the ID number and the name is risky because anyone who stole (or even took a photo of) an ID can be positively verified; this will only confirm knowledge. In New Zealand, regulator suggests using biometric verification as a supplement to verification via reliable database (Identity Verification Code of Practice - Explanatory Note, 2017), but, as we discuss later, this complicates the process and makes it more expensive. The cheaper alternative might to verify diverse information that cannot be obtained from one source (thus confirming the possession – that the person actually has access to the personal documents). One example is Russia where SDD requires not only ID number and name but also additional identifiers which can be either a personal tax number or a social security number or a number of the medical insurance certificate. Neither of the additional identifiers is printed on the ID, and they are very rarely kept together. The same principle applies in the UK where "corroborative" information is seen as one of the alternatives to biometrics (The Joint Money Laundering Steering Group, 2017).

The need for two-factor authentication for a reliable confirmation of identity also raises the question about the new types of IDs. In some jurisdictions, authorities try to implement plastic IDs as identification documents. There is a temptation to make them universal and put as much information on the card as possible: name, date of birth, identification numbers, etc. Although this might help combat cluttered wallets, this creates additional risks of impersonation and complicates the implementation of remote CDD using simple verification methods.

5.3 Biometrics

Biometrics is a hot topic among the AML/CFT professionals. It promises higher level of protection and reliability. But it also has downsides; it is costly and sometimes requires using special hardware by the consumers (e.g. fingerprint scanners). The CDD process that uses biometrics can also be disaggregated by using the IVCid model.

Possibly, the largest markets with the biometrics-based CDD mechanisms are India and Russia.

As seen in Russian biometrics system, the biometrics is only a factor in the confirmation of identity (inherence). Here, biometric data (digital photo and a voice print) and ID information are stored in a central database coupled with an e-government website (ESIA). When an individual wants to go through remote CDD, he/she logs in ESIA using biometrics and login/password and authorizes the transfer of personal information to the financial institution. Therefore, the verification is done at the ESIA level, while confirmation is still based on knowledge (login/password) and inherence (biometrics). Similar approach is taken in India where biometric/OTP verification is required in addition to presenting Aadhaar card (The Economic Times, 2018).

The biometrics is a costly affair and can be replaced just by another element in two-factor authentication. For example, in Belarus, login and password (knowledge) and one-time SMS

password (possession) are used, instead of inherence, for the remote identification procedure that looks very much like Russian.

It could be argued that the two-factor authentication might be excessive when biometrics is involved. However, using only biometric factor might create additional risks such as if biometric information is compromised so is the whole database. This is especially risky, considering the irrevocability of biometrics.

5.4 Using electronic signatures

Electronic signatures (e-signature) are a popular topic for discussion when talking about the new CDD methods. Although it works in a very limited number of jurisdictions, this solution is often viewed as preferable by many decision-makers. The attraction is understandable. E-signature can act as a remote alternative to face-to-face interaction. But using it for remote CDD is tricky. The IVCid model explains why.

The identification stage is simple, as we described previously, and does not require e-signature per se. For the verification purposes, the reliable source of information is e-signature certificate itself. Any usage of e-signature, whether for the CDD purposes, also requires the two-factor authentication (e.g. token – possession and pin-code/OTP – knowledge).

There is one potential drawback, that is, to be a reliable source of information, the e-signature certificate needs to contain all data required according to the AML/CFT laws. This is not always the case. From the practical point of view, e-signature tokens might be expensive (customers usually, with few exceptions, need to pay for an annual renewal of certificates) and hard to use (e.g. tokens cannot be used with devices without USB ports). Introduction of“cloud-based” e-signatures can only partially offset these problems.

6. Conclusion

The FATF Recommendations and guidance contain a very broad description of the best practices. To be universal, they have to be based on pure principles, but the actual CDD in a financial institution cannot be. This is a set of well-described procedures that the bank officer needs to follow. Moreover, in countries with rule-based regulations, these procedures are even prescribed in laws.

The IVCid model provides a practical reference point for the analysis of the existing CDD procedures and can be a helping tool for devising new ones. Because the model is technology-neutral, it can be applied to both remote and face-to-face CDD procedures. The IVCid model also provides some valuable theoretical and applied insights.

All the CDD procedures work the same in practice. Whether they are paper-based, electronic, face-to-face or remote, they all contain the same stages, namely, identification (collection of information), verification (verifying the veracity of information) and confirmation of identity (using a two-factor authentication). The IVCid model is technology- neutral and allows the

regulators and financial institutions to devise a process that is more cost-effective, relevant and reliable in their particular situation without necessarily trying to copy others' experiences. In essence, three stages of the IVCid model allows for the "modular" CDD approach, as seen in Table II.

The IVCid model shows that the choice of a successful CDD procedure boils down to two essential questions. First is ensuring the availability of reliable source of information and deciding which sources to consider reliable. Second is ensuring an effective two-factor authentication which will depend on existing infrastructure – availability of biometrics database, existence of a trusted third party, possession of unique identifiers (SIM cards, e-signature tokens, etc.), etc. Unlike these issues, the collection of information seems to be the simplest stage in terms of implementation.

Table 2 – Forms of IVCid model elements

Identification	Verification	Confirmation of identity
Verbal (in person)	Paper-based state-issued ID	Possession (documents, SIM cards, etc.)
Verbal (remotely)	Paper-based non-state-issued documents	Inherence (biometrics)
Written (in person)	State-owned database	Knowledge (passwords, pincodes, etc.).
Written (remotely)	Credit bureau	
	Specifically created database	
	Mobile network operators	

From the practical point of view, the IVCid model draws attention to at least the following issues. First, distribution of "universal IDs" where all confidential identifiers are printed on an ID card for the sake of "convenience." This compromises the usage of such IDs, especially in the non-face-to-face CDD. Second, jurisdictions need a clear understanding of which sources of information should be considered reliable. Finally, when implementing the remote CDD or SDD reforms, the regulators and financial institutions may be advised to look at what their countries already have in terms of reliable databases and two-factor authentication, as this may suggest a cheaper alternative to more expensive and popular options. We believe that the FATF Guidance may benefit from incorporating the IVCid model, as it is technology- and business-neutral. At the moment of writing, the FATF has mentioned a similar approach that is draft guidance on digital identity where the stages of checking the veracity of information is separated from the confirmation that the ID relates to the person (FATF, 2019). However, it focuses solely on digital identity solution and proofing/enrolment processes.

The IVCid model also suggests avenues for further research. First, more research is needed to understand the formal factors that affect the reliability of a source of information. Second, more comparative research is required to understand the strengths and weaknesses of biometric-based

or e-signature-based solutions. Finally, more research might be needed to understand which factors in the IVCid model might be more beneficial to financial inclusion than others.

Note

1. Although exact terms may vary from jurisdiction to jurisdiction, the term "CIP" is derived from the US practice, while in other countries, it may be called "identification" or even not formally outlined as a separate element of CDD.

References

1. Alliance for Financial Inclusion (2016), *Benchmarking financial inclusion in Fiji, Samoa, and Solomon Islands: Findings from the first national demand side surveys*, Pacific Financial Inclusion Programme, p. 7, available at: https://www.afi-global.org/sites/default/files/publications/piri_cross_country_report_final_uploaded.pdf

2. Alliance for Financial Inclusion (2019), *KYC Innovations, Financial Inclusion and Integrity in Selected AFI Members Countries,* AFI Special Report, available at: https://www.afi-global.org/sites/default/files/publications/2019-03/KYC-Innovations-Financial-Inclusion-Integrity-Selected-AFI-Member-Countries.pdf

3. *Amended Identity Verification Code of Practice 2013*, 2017, available at: https://www.fma.govt.nz/assets/Guidance/AML-CFT-identity-verification-code-of-practice-2013.pdf

4. AUSTRAC (2019), *Customer identification: Know your customer (KYC)*, available at: https://www.austrac.gov.au/business/how-comply-and-report-guidance-and-resources/customer-identification-and-verification/customer-identification-know-your-customer-kyc

5. AUSTRAC (2020), *Identifying customers who don't have conventional forms of ID*, available at: https://www.austrac.gov.au/business/how-comply-and-report-guidance-and-resources/customer-identification-and-verification/identifying-customers-who-dont-have-conventional-forms-id

6. Banerjee, S. (2016), *Aadhaar: Digital Inclusion and Public Services in India*, World Development Report, available at: http://pubdocs.worldbank.org/en/655801461250682317/WDR16-BP-Aadhaar-Paper-Banerjee.pdf

7. Basel Committee on Banking Supervision (2001), *Customer due diligence for banks*, Bank for International Settlements, available at: https://www.bis.org/publ/bcbs85.pdf

8. Basel Committee on Banking Supervision (2017), *Sound management of risks related to money laundering and financing of terrorism*, Bank for International Settlements, available at: https://www.bis.org/bcbs/publ/d405.pdf

9. Commission Delegated Regulation (EU) 2018/389 of 27 November 2017 supplementing Directive (EU) 2015/2366 of the European Parliament and of the Council with regard to regulatory technical standards for strong customer authentication and common and secure open standards of communication, *Official Journal of the European Union,* 2018, L 69, 13.03, pp. 23-43.

10. De Koker, L. (2006), "Money Laundering Control and Suppression of Financing of Terrorism: Some Thoughts on the Impact of Customer Due Diligence Measures on Financial Exclusion", *Journal of Financial Crime*, Vol. 13 No. 1, pp. 26-50.

11. De Koker, L. (2014), "The FATF's Customer Identification Framework: Fit for Purpose?", *Journal of Money Laundering Control*, Vol. 13 No. 3, pp. 281-295, DOI: 10.1108/JMLC-01-2014-0003

12. Demetis, D. and Angell, I. (2007), "The risk-based approach to AML: representation, paradox, and the 3rd directive", *Journal of Money Laundering Control*, Vol. 10 Issue 4, p. 427 (pp.412-428).

13. Directive (EU) 2015/2366 of the European Parliament and of the Council of 25 November 2015 on payment services in the internal market, amending Directives 2002/65/EC, 2009/110/EC and 2013/36/EU and Regulation (EU) No 1093/2010, and repealing Directive 2007/64/EC (2016), *Official Journal of the European Union*, 016 L 337, 23.12, pp. 35-127.

14. Dostov, V., Shust, P. and Kozyreva, A. (2018), "Non-face-to-face customer due diligence in Russia: The status quo", *Financial Regulation International*, Vol. 20 No. 10.

15. Duyne, P., Harvey, J. and Gelemerova, L. (2018*), The Critical Handbook of Money Laundering: Policy, Analysis and Myths*, Palgrave Macmillan, p. 311, DOI: 10.1057/978-1-137-52398-3

16. FATF (1990), *The Forty Recommendations of the Financial Action Task Force on Money Laundering*, available at: https://www.fatf-gafi.org/media/fatf/documents/recommendations/pdfs/FATF%20Recommendations%201990.pdf

17. FATF (2012-2019)*, International Standards on Combating Money Laundering and the Financing of Terrorism & Proliferation*, The FATF Recommendations, available at: www.fatf-gafi.org/recommendations.html

18. FATF (2013-2017), Anti-money laundering and terrorist financing measures and financial inclusion - With a supplement on customer due diligence, FATF Guidance, p. 10, available at: www.fatf-gafi.org/publications/financialinclusion/documents/financial-inclusion-cdd-2017.html

19. FATF (2017)*, Anti-Money Laundering and Terrorist Financing Measures and Financial Inclusion*, FATF Guidance, available at: https://www.fatf-gafi.org/media/fatf/content/images/Updated-2017-FATF-2013-Guidance.pdf

20. FATF (2019), *Draft Guidance On Digital Identity*, available at: https://www.fatf-gafi.org/publications/fatfrecommendations/documents/consultation-digital-id-guidance.html

21. Gelb, A. (2016), *Balancing Financial Integrity with Financial Inclusion: The Risk-Based Approach to "Know Your Customer"*, CGD Policy Paper 74, Washington DC: Center for Global Development, available at: https://www.cgdev.org/sites/default/files/CGD-Policy-Paper-Gelb-KYC-Financial-Incl.pdf

22. GIABA (2018), *Know Your Customer / Customer due Diligence Measures and Financial Inclusion in West Africa*, An Assessment Report, available at: https://www.giaba.org/media/f/1062_FInal%20KYC-CDD%20Assessment%20Report%20Published.pdf

23. Gill, M. and Taylor, J. (2004), "Preventing Money Laundering or Obstructing Business? Financial Companies' Perspectives on 'Know Your Customer' Procedures", *The British Journal of Criminology*, Vol. 44 No. 4, pp. 588-589.

24. *Identity Verification Code of Practice - Explanatory Note (2017)*, available at: https://www.rbnz.govt.nz/-/media/ReserveBank/Files/regulation-and-supervision/anti-money-laundering/guidance-and-publications/Identity%20Verification%20Code%20of%20Practice%20-%202017%20Explanatory%20Note.pdf

25. Kipkemboi, K., Woodsome, J. and Pisa, M. (2019), *Overcoming the Know Your Customer Hurdle: Innovative Solutions for the Mobile Money Sector*, GSM Association, available at: https://www.gsma.com/mobilefordevelopment/wp-content/uploads/2019/02/Overcoming-the-KYC-hurdle-Innovative-solutions-for-the-mobile-money-sector.pdf

26. *Law No 115-FZ "On countering the legalization (laundering) of criminally obtained incomes and the financing of terrorism"(2001),* Art. 7, par 1.12 (2), available at: https://cbr.ru/Content/Document/File/29897/115-FZ.pdf

27. Mugarura, N. (2014), "Customer due Diligence (CDD) Mandate and the Propensity of its Application as a Global AML Paradigm", *Journal of Money Laundering Control*, Vol. 17 No. 1, pp. 76-95, https://doi.org/10.1108/JMLC-07-2013-0024

28. Mulligan, D. (1998), "Know Your Customer Regulations and the International Banking System: Towards a Self-Regulatory Regime", *Fordham International Law Journal*, Vol. 22 No. 5, p. 2372.

29. Pol, R. (2018), "Anti-Money Laundering Effectiveness: Assessing Outcomes or Ticking Boxes?", *Journal of Money Laundering Control*, Vol. 21 No. 2, p. 223 (pp. 215-230).

30. Smet, D.D. and Mention, A. (2011), "Improving auditor effectiveness in assessing KYC/AML practices: Case study in a Luxembourgish context", *Managerial Auditing Journal*, Vol. 26 No. 2, p. 183 (pp. 182-203).

31. Sotande, E. (2018), "The Regime against Money Laundering: a Call for Scientific Modelling", *Journal of Money Laundering Control*, Vol. 21 No. 4, pp. 584-593, DOI: 10.1108/JMLC-11-2017-0066

32. *Statute on Customer Due Diligence (2018),* Par. 16, available at: http://cbd.minjust.gov.kg/act/view/ru-ru/12934?cl=ru-ru

33. The Economic Times (2018), "Banks opening accounts using Aadhaar copy without biometric/OTP check will be liable for loss: UIDAI", Sep 12, available at: https://economictimes.indiatimes.com/wealth/personal-finance-news/banks-opening-accounts-using-aadhaar-copy-without-biometric/otp-check-will-be-liable-for-loss-uidai/articleshow/65486310.cms?utm_source=contentofinterest&utm_medium=text&utm_campaign=cppst

34. The Joint Money Laundering Steering Group (2017), *Prevention of money laundering/combating terrorist financing*, 2017 Revised Edition, p. 90. Available at: http://www.jmlsg.org.uk/bba/jsp/polopoly.jsp?d=749

35. The World Bank Group (2017), *Global Financial Inclusion and Consumer Protection Survey*, Report, International Bank for Reconstruction and Development, p.27, available at: https://openknowledge.worldbank.org/bitstream/handle/10986/28998/122058.pdf

36. Theodorou, Y. and Yongo, E.(2018), *Access to Mobile Services and Proof-of-Identity: Global Policy Trends, Dependencies and Risks,* GSM Association, available at: https://www.gsma.com/mobilefordevelopment/wp-content/uploads/2018/02/Access-to-Mobile-Services-and-Proof-of-Identity.pdf

37. Turner, S. and Bainbridge, J. (2018), "An Anti-Money Laundering Timeline and the Relentless Regulatory Response", *The Journal of Criminal Law*, Vol. 82 No. 3, p. 231 (215-231), DOI: 10.1177/0022018318773205

38. Yasin, N.M. (2015), "Statutory obligations for banks to comply with the anti-money laundering legislation in Malaysia: Lessons from the United Kingdom", *Journal of Banking Regulation*, Vol. 16, pp. 326-344, DOI: 10.1057/jbr.2014.21