iCard

ДО
НАРОДНО СЪБРАНИЕ
НА РЕПУБЛИКА БЪЛГАРИЯ

На вниманието на:

Комисия по вътрешна сигурност и обществен ред (водеща)

Комисия за контрол над службите за сигурност, прилагането и използването на специалните разузнавателни средства и достъпа до данните по Закона за електронните съобщения

Комисия по бюджет и финанси

Комисия по правни въпроси

Комисия по икономическа политика и туризъм

Комисия по европейските въпроси и контрол на европейските фондове

КОПИЕ:

ДЪРЖАВНА АГЕНЦИЯ „НАЦИОНАЛНА СИГУРНОСТ"
САД „ФИНАНСОВО РАЗУЗНАВАНЕ"
ДИРЕКТОР НА САД ФР - ДАНС Е.ЕВГЕНИЕВ

От
Айкарт АД
(предишно наименование „Интеркарт Файнанс" АД)
ЕИК: 175325806
бул. Джеймс Ваучер 76А,
БЦ Хил Тауър, ет. 8
гр. София, 1407

Дата: 12.10.2017 г.

Относно: Проект на нов Закон за мерките против изпиране на пари и текстове, които са в противоречие с Директива (ЕС) 2015/849 на Европейския парламент и на Съвета от 20 май 2015 година за предотвратяване използването на финансовата система за целите на изпирането на пари и финансирането на тероризма („4-та АМЛ Директива").

Уважаеми дами и господа,

Във връзка с приетия на първо четене на 06.10.2017 г. законопроект за мерките срещу изпирането на пари (ЗМИП), предоставяме на Вашето внимание становище по текстовете на предложения закон от името на „Айкарт" АД, в качеството му на дружество за електронни пари, лицензирано от БНБ и задължено лице, според законопроекта

Проектът за нов ЗМИП следва да транспонира Директива (ЕС) 2015/849 на Европейския парламент и на Съвета от 20 май 2015 година за предотвратяване използването на финансовата система за целите на изпирането на пари и финансирането на тероризма (по-нататък „Директива 2015/849/ЕС" или „4-та АМЛ Директива").

С настоящото писмо желаем да Ви обърнем внимание относно някои текстове от Законопроекта на ЗМИП, които считаме че следва да бъдат изменени с оглед на това, че тяхното включване в закона в сегашния им вид би довело до значителни затруднения в прилагането на последния, а други са в противоречие с текстовете на Директива 2015/849/ЕС и следва да бъдат коригирани, за да се транспонира Директивата надлежно в българското законодателство:

1. Чл. 24 от Проекта за ЗМИП е в противоречие с императивната норма на чл.12 от Директива 2015/849/ЕС:

Съгласно член 12 от Директива 2015/849/ЕС: „Чрез дерогация от член 13, параграф 1, първа алинея, букви а), б) и в), и член 14 и въз основа на подходяща оценка на риска, която показва наличието на **ниска степен на риск,** дадена държава членка може да разреши на ***задължените субекти да не прилагат определени мерки за комплексна проверка*** на клиента по отношение на електронни пари, **когато са изпълнени всички посочени по-долу условия за намаляване на риска (кумулативно дадени условия за нисък риск на платежния инструмент/електронни пари):**

а) платежният инструмент **не е презаредим** или **има максимален месечен лимит** на плащанията по сделки от 250 **EUR,** който може да се използва само в съответната държава членка;
б) максималната електронно съхранявана сума не надхвърля 250 EUR;
в) платежният инструмент се използва изключително за закупуване на стоки или услуги;
г) платежният инструмент не може да се захранва с анонимни електронни пари;
д) емитентът осъществява подходящо наблюдение на сделките или деловите взаимоотношения, позволяващо разкриването на необичайни или съмнителни сделки.

2. Държавите членки гарантират, че предвидената в параграф 1 дерогация не се прилага в случай на обратно изкупуване в брой или теглене в брой на паричната стойност на електронните пари, когато възстановената сума надвишава 100 EUR."

Настоящата редакция на чл.24 от Проекта на ЗМИП гласи:

„Чл. 24. (1) Издателите на електронни пари и техните представители прилагат мерките за комплексна проверка на клиента по отношение на електронни пари, когато:
а) платежният инструмент е презаредим или има максимален месечен лимит на плащанията по сделки над левовата равностойност на 150 евро или тяхната равностойност в друга валута, който може да се използва и в чужбина; или
б) максималната електронно съхранявана сума надхвърля левовата равностойност на 150 евро или тяхната равностойност в друга валута; или

в) платежният инструмент не се използва за други цели освен закупуване на стоки или услуги; или
г) платежният инструмент може да се захранва с анонимни електронни пари; или
д) при обратно изкупуване в брой или теглене в брой на паричната стойност на електронните пари възстановената сума надвишава левовата равностойност на 50 евро или тяхната равностойност в друга валута; или
е) при платежни операции, свързани със средства за дистанционна комуникация по смисъла на Закона за платежните услуги и платежните системи." (край на цитата).

На първо място прави впечатление „обърнатата" логика на текста в сравнение с този в Директивата. Това води до юридическия нонсенс в буква а) на чл. 24, ал. 1, която гласи, че за да не се приложи комплексна проверка на клиента по отношение на електронни пари (per argumentum a contrario) платежният инструмент следва да е непрезаредим и да има максимален месечен лимит на плащанията до 150 евро. Това обаче изменя смисълът на чл. 12 от Директивата, съгласно който, за да не се приложи комплексна проверка спрямо клиента, платежният инструмент за електронни пари следва **да е непрезаредим** или **да е презаредим с месечен лимит** на плащанията до 250 евро. Това става съвсем явно при преглед на английския текст на Директивата „the payment instrument is not reloadable, or has a maximum monthly payment transactions limit of EUR 250 which can be used only in that Member State".

Систематичното тълкуване на точка а) и точка б) също потвърждава този извод - нелогично е непрезаредим платежен инструмент с максималната електронно съхранявана сума до 150 евро да има възможността да има максимален месечен лимит на плащанията по сделки над левовата равностойност на 150 евро. Логиката на Директивата е съвсем ясна - за да се приложи дерогацията, непрезаредимият инструмент не може да има максимално електронно съхранявана сума над 250 евро, а в случай, че е презаредим - неговият максимален месечен лимит на плащанията не може да надхвърля 250 евро.

На следващо място, разпоредбата на чл.12 от Директивата е изключение от общото правило за задължение на задължените субекти да прилагат определени мерки за комплексна проверка и Държавите членки не могат да се отклоняват при нейното транспониране, освен ако отклонението не въвежда по-високи изисквания за намаляването на рисковете. Разбираме, че въвеждането на лимити от 150 евро за плащане на стоки или услуги (в Директивата е 250 евро) и съответно 50 евро за обратно изкупуване или теглене в брой (в Директивата е 100 евро) е продиктувано от желанието на българския законодател да наложи по-високи изисквания от предвидените в Директивата.

Въпреки това, „Айкарт" АД призовава българският законодател да преосмисли своята позиция относно въвеждането на по-стриктни мерки от наложените в Директивата.

На първо място това ще постави българските дружества за електронни пари в по-неблагоприятно пазарно положение от своите конкуренти в останалите държави-членки на ЕС.

На второ място това по-стриктно третиране спрямо българските издатели на електронни пари е неоправдано и непоследователно. Електронните пари никога не са били идентифицирани от ДАНС или останалите компетентни органи в областта на

противодействие на изпирането на пари в Република България като криещи повишен риск. Неясно е с какво българските издатели на електронни пари крият по-голям риск от улесняването на проникването на парични средства, добити по престъпен начин или от използването на финансовата система за финансиране на тероризъм, от останалите издатели на електронни пари в рамките на Европейския съюз.

Поради това предлагаме текстът на чл. 24 да бъде приведен изцяло в съответствие с този на чл. 12 от Директивата:

„чл. 24 (1) Издателите на електронни пари и техните представители не прилагат мерките за комплексна проверка на клиента по отношение на електронни пари, когато са изпълнени всички посочени по-долу условия за намаляване на риска:

а) платежният инструмент не е презаредим или има максимален месечен лимит на плащанията по сделки от 250 EUR или паричната им равностойност в лева;

б) максималната електронно съхранявана сума по платежния инструмент не надхвърля 250 EUR или паричната им равностойност в лева;

в) платежният инструмент се използва изключително за закупуване на стоки или услуги;

г) платежният инструмент не може да се захранва с анонимни електронни пари;

д) издателят на електронни пари осъществява подходящо наблюдение на сделките или деловите взаимоотношения, позволяващо разкриването на необичайни или съмнителни сделки.

(2). В случай, платежният инструмент не може да се използва извън територията на Република България, максималната електронно съхранявана сума по платежния инструмент по буква б) на предходната алинея може да бъде по-голяма от 250 EUR или паричната им равностойност в лева, но не повече от 500 EUR или паричната им равностойност в лева.

(3) Предвидената в ал. 1 дерогация не се прилага в случай на обратно изкупуване в брой или теглене в брой на паричната стойност на електронните пари, когато възстановената сума надвишава 100 EUR или паричната им равностойност в лева.

2. Чл. 53, ал.1 от Проекта за ЗМИП е стъпка назад в българското законодателство относно противодействието на изпирането на пари.

Според предложената редакция на чл. 53, ал.1 *„Идентифицирането на физическите лица се извършва чрез представяне на официален документ за самоличност и **снемане на копие от него."***

Съгласно действащия към момента ЗМИП:

„Чл. 6. (1) (Изм. -ДВ, бр. 54 от 2006 г.) Идентифицирането на клиентите и проверката на тяхната идентификация се извършват:

[..-]

*2. за физическите лица - **чрез представяне** на официален документ за самоличност и регистриране на неговия вид, номер, издател, както и на името, адреса, единния граждански номер, а за физическите лица, имащи качеството на едноличен търговец - и чрез представяне на документите по т. 1."*

Видно от горното снемането на копие от официален документ на физическите лица към момента не се изисква. Считаме, че това ново изискване е неоправдано утежняващо и няма да доведе до никаква реална полза в постигането на целите на законопроекта. Предлагаме последната част от изречението „и снемане на копие от него." да отпадне.

3. Чл. **55,** ал. **2** от Проекта на ЗМИП показва неправилно тълкуване на ситуации с повишен риск при случай на дистанционно установяване на взаимоотношения

Съгласно предложената редакция на чл. 55, ал. 2 от Проекта на ЗМИП: *„При установяване на делови взаимоотношения или осъществяване на случайна операция или сделка чрез електронно изявление,* ***електронен документ или електронен подпис,*** *или чрез друга форма без присъствието на клиента лицата по чл. 4 извършват проверка на събраните идентификационни данни чрез използване на два или повече от способите по ал. 1. Допълнителни мерки за удостоверяване истинността на идентификационните данни на клиента могат да се определят с правилника за прилагане на закона."*

Действително, съгласно Приложение III от Директивата, подобни ситуации са определени като имащи потенциално по-висок риск по член 18, параграф 3. Въпреки това, наличието на електронен документ или електронен подпис е фактор, който **намаля риска,** видно от т. 2, буква в) на Приложение III от Директивата, която гласи:

,,в) индиректни делови взаимоотношения или сделки **без определени предпазни мерки,** като например електронни подписи" (английският текст на директивата е дори по-ясен: *„non-face-to-face business relationships or transactions,* ***without certain safeguards, such as electronic signatures"***

Следователно, в случай че предпазни мерки са налице, като например електронни подписи - тази ситуация не следва да се третира като такава с потенциално по-висок риск по член 18, параграф 3.

Поради горното, предлагаме частта „електронен документ или електронен подпис" от чл. 55, ал. 2, да отпадне от Проекта.

4. Чл. **56,** ал. **1** от Проекта на ЗМИП неоправдано облагодетелства единствено кредитните институции (банки) и ограничава правото на задължените лица да разчитат на предходна верификация, извършена от трети лица, задължени по AML законодателството, което е в противоречие на изискванията на Директивата.

Съгласно предложената редакция на чл. 56, ал. 1 от Проекта на ЗМИП: *„Лицата по чл. 4, т. 1-3, 5 и 8-11 могат да се позоват на предходно идентифициране на клиента,* ***извършено от кредитна институция*** *за целите на чл. 10, т. 1 и 2, при наличие на следните кумулативни условия:*

1. седалището на извършилата идентифицирането ***кредитна институция*** *е в Република България, в друга държава членка или в трета държава, която отговаря на условията на чл. 27"*

Неясно е защо в предложения законопроект се дава възможност за позоваване на предходна комплексна проверка, извършена единствено от кредитна институция. Това противоречи на логиката на Директивата, която гласи в чл. 25 и чл. 26:

„Член 25

Държавите членни могат да позволят на задължените субекти да възлагат на ***трети лица*** *функции по спазване на изискванията за комплексна проверка на клиента, предвидени в член 13, параграф 1, първа алинея, букви а), б) и в). Въпреки това, крайната отговорност за спазването на тези изисквания се носи от задължения субект, който възлага функции на трето лице.*

Член 26

1. За целите на настоящия раздел ***„трети лица"*** *означава* ***задължени субекти, изброени в член*** *2, организации или федерации, членуващи в тези задължени субекти, или други институции и лица, намиращи се в държава членка или в трета държава:*

а)които прилагат изисквания за комплексна проверка на клиента и съхраняване на информация, които съответстват на предвидените в настоящата директива, и

б)във връзка с изпълнението на изискванията, установени в настоящата директива подлежат на надзор, който се осъществява по начин съответстващ на глава VI, раздел 2.

2. Държавите членки забраняват на задължените субекти да разчитат на трети лица, установени във високорискови трети държави. Държавите членки могат да освобождават клонове и мажоритарно притежавани дъщерни предприятия на задължени субекти, установени в Съюза, от тази забрана, когато тези клонове и мажоритарно притежавани дъщерни предприятия спазват изцяло политиките и процедурите в рамките на групата в съответствие с член 45."

Видно от горното, задължените субекти, прилагащи мерките на закона следва да могат да се позовават на предходна комплексна проверка, извършена от други задължени субекти. Кредитните институции са само един от 35-те вида задължени лица съгласно чл. 4 от Проекта на ЗМИП.

5. В Проекта на ЗМИП не е съобразено, че Четвъртата AML Директива е от значение и за ЕИП.

Съгласно §1, т. 6 от Законопроекта *„Държава членка" е държава, която е членка на Европейския съюз."*

За целите на общностното законодателство в областта на прилагането на мерките срещу изпиране на пари и финансиране на тероризма, под „държава членка" винаги се има предвид държава членка на ЕС и/или на ЕИП. Това е видно и от самото заглавие на директивата, което включва пояснението „(текст от значение за ЕИП)"

С оглед на гореизложеното, предлагаме §1, т. 6 от Законопроекта да бъде със следната редакция: *„Държава членка" е държава, която е членка на Европейския съюз или на Европейското Икономическо Пространство"*

6. **Проверка чрез видео разговор („видео верификация") като един от способите за комплексна проверка.**

Множество дружества за електронни пари и платежни институции в Европа, задължени лица по смисъла на ЗМИП, откриват сметки и встъпват в отношение именно неприсъствено със

своите клиенти, прилагайки подобна разширена комплексна проверка. Това вече не представлява необичайна практика, а напротив, приема се за адекватен подход за справяне с по-високия риск при този тип *индиректни делови взаимоотношения („non-face-to-face").* В подкрепа на този извод е и параграф 19 от Преамбюла на Директивата, който сочи, *че* ***„Новите технологии предлагат ефективни от гледна точка на времето и разходите решения за дружествата и за клиентите и поради това следва да се вземат предвид при оценката на риска. Компетентните органи и задължените субекти следва да действат активно в борбата с новите и иновативните способи за изпиране на пари."***

Българските дружества за електрони пари и платежни институции желаят да се конкурират с европейските онлайн банки като PayPal (Люксмебург) и Number26 (Германия) и дружества за електронни пари и платежни институции като Skrill (Англия), Neteller (Англия), iZettle (Швеция), Sumup (Англия), Paysera (Литва) като въведат иновативните подходи, прилагани от последните, във връзка с извършването на видео верификация на техните клиенти.

Поради това, с настоящото „Айкарт" АД желае да предложи на българският законодател в законопроекта на ЗМИП или в правилника за прилагане, който предстои да бъде приет, да бъдат включени изрични законови текстове, регламентиращи този вид способ за комплексна проверка.

Като пример желаем да предложим процедурата на Федералния Надзорен Орган на ФР Германия (Bundesanstalt fur Finanzdienstleistungsaufsicht - BAFIN), описана подробно в Circular 3/2017 (GW) - video identification procedures на https://www.bafin.de/SharedDocs/Veroeffentlichungen/EN/Rundschreiben/2017/rs_1703gw_videoident_en.html, която прилагаме преведена от оторизирана преводаческа агенция (Приложение № 1)

В приложение на точно тази процедура немската онлайн банка Number26 (www.n26.com). извършва идентификация на своите клиенти единствено чрез приложение на процедурата, като идентифицира и верифицира клиенти физически лица от различни страни в Европа.

Тази процедура е описана подробно и в Правилника за прилагане на мерките против изпиране на пари на малтийския регулаторен орган Financial Intelligence Action Unit на, достъпна на http://www.fiumalta.org/library/PDF/misc/27.01.2017-Implementing%20Procedures%20Part%2QI2017.pdf

Считаме, че такава процедура следва да бъде въведена в текстовете на Законопроекта или в бъдещия Правилник за прилагане на ЗМИП, тъй като тя отразява последните постижения в Европа в технологията на засилените мерки против изпиране на пари и финансиране на тероризъм и дава възможност на задължените лица да предоставят на компетентните органи видеозапис на физическите лица, заедно с много добри копия на техните документи за самоличност.

Приложения:

Приложение № 1: Превод на български език на Циркулярна нота 3/2017 г. (GW) - процедури за видео идентификация (издадена от BAFIN)

С Уважение:

Деян Добрев
Изпълнителен д

Изготвено с помощта H a S C ^ ^ D ^

Адвокатско Дружество

„Прокопиева § Савчева"
www.eu-bg.com
Адвокат Вася Прокопиева
Адвокат Таня Савчева
Адвокат Мартин Емилов

Циркулярна нота 3/2017 г. (GW) – процедури за видео идентификация

Референтен номер GW 1-GW 2002-2009/0002 Дата: 10 април 2017 г.

Изисквания за използване на процедури за видео идентификация (Справка: Циркулярна нота 1/2014 г., Точка III от 5 март 2014 г.)

На тази страница:

Настоящата циркулярна нота е предназначена за: кредитни институции, институции за финансови услуги, платежни институции, институции за електронни пари, предприятия и лица по смисъла на Раздел 2 (1) №. 2c от Закона срещу прането на пари на Германия (Geldwaschegesetz - GwG), дружества за управление на активи, браншове на фирми за управление в ЕС, чуждестранни дружества за управление на алтернативни инвестиционни фондове, чуждестранни дружества за управление на алтернативни инвестиционни фондове, за които Федерална Република Германия е референтна държава членка и които са под надзора на Германския федерален орган за финансов надзор (Bundesanstalt fur Finanzdienstleistungsaufsicht - BaFin) съгласно Раздел 57 (1), изречение 3 от Германския инвестиционен кодекс

(Kapitalanlagegesetzbuch - KAGB), застрахователни предприятия, предлагащи животозастрахователни договори или застрахователни договори за злополука с възстановяване на премии, както и финансови холдинги и смесени финансови холдинги във Федерална Република Германия.

Справка: Циркулярна нота 1/2014 г.. Точка III от 5 март 2014 г.

A. Идентификация на физически лица, които присъстват чрез процедури за видео идентификация

Германското Федерално министерство на финансите (Bundesministerium der Finanzen - BMF) запазва тълкуването си във връзка с обхвата на засилената надлежна проверка на клиента в случаи на идентификация, която не се извършва лице в лице, съгласно Раздел 6 (2) № 2 от германския Закон срещу прането на пари, посочено в Циркулярна нота 1/2014 г. от 5 март 2014 г. Тази процедура не противоречи на четвъртата Директива за предотвратяване използването на финансовата система за целите на изпирането на пари и финансирането на тероризма (Директива (ЕС) 2015/849), според която дори случаите на непряка идентификация не представляват повишен риск в основата си.

Тълкуването на германското Федерално министерство на финансите гласи, че в случаи на видео идентификация сензорното възприятие на (физическите) лица, участващи в процеса на идентификация, е възможно независимо от физическото разстояние, тъй като лицето за идентификация и служителят са един срещу друг, „лице в лице" по време на видео сесията и общуват един с друг.

Идентифицирането в тези случаи следователно се основава на общите изисквания за идентификация на клиентите за физически лица, изложени в Раздел 3 (1) № 1 във връзка с Раздел 4 (1), (3) № 1 и (4) № 1 от германския Закон срещу прането на пари.

Видео идентификацията на юридически лица или партньорства от друга страна е невъзможно. Процедурата за видео идентифициране обаче може да се използва в случаи, когато трябва да се потвърди самоличността на правен или упълномощен представител.

Тази циркулярна нота заменя Точка III от Циркулярна нота 1/2014 г. от 5 май 2014 г. във връзка с видео идентификацията. Тя адаптира процедурата към текущите изисквания във връзка със сигурността и приложимостта, като следователно повишава нивото на сигурността в частност.

Поради това използването на процедури за видео идентификация вече се основава само и единствено на настоящата циркулярна нота и на изискванията, изложени по-долу, които трябва да се спазват кумулативно и в своята цялост. Въз основа на тези изисквания процедурата за видео идентификация може да се използва от всички лица, които са обект на Закона срещу прането на пари и които са под моя надзор.

Процедурата за видео идентификация, описана в настоящата Циркулярна нота, следва да се оцени, ако има причина за подобна оценка (например известни са инциденти, свързани със сигурността), но при всички случаи не по-късно от три години след влизането в сила на Циркулярната нота. Процедурата трябва да се оцени, за да се провери дали изискванията за спазването й съгласно законодателството за пране на пари все още са в съответствие с нивото на технологичен напредък и опита, придобит с процедурата, и дали са необходими допълнителни корекции или изисквания. Резултатът от тази оценка е обвързващ във връзка със самата процедура, както и с всякакви изисквания за корекции, които може да възникнат.

B. Изисквания на Закона за мерките срещу изпирането на пари във връзка с извършване на видео идентификация

I. Идентификация от обучени служители

Видео идентификацията може да се извършва само от подходящо обучени служители на задълженото лице или на трета страна, на която задълженото лице е възложило изискването за идентификация на клиенти съгласно Раздел 7 (2) на германския Закон срещу прането на пари или с което задълженото лице се е ангажирало съгласно Раздел 7 (1) от германския Закон срещу прането на пари. Не се позволява по-нататъшно делегиране, вторично делегиране или ангажиране на трета страна от трета страна по смисъла на Раздел 7 (1) на германския Закон срещу прането на пари.

Въпросните служители трябва най-малко да са запознати с характеристиките на допустимите документи за процедурата за видео идентификация, които може да се проверят чрез въпросната видео идентификация (включително приложимите методи за проверка), заедно с често срещаните възможности за фалшифициране и следва да са запознати с приложимото законодателство за изпирането на пари и защита на данните, както и изискванията, изложени в настоящата Циркулярна нота. Трябва да

има налична подходяща документация за приетите документи, техните характеристики, които могат да бъдат проверени, и съответните мерки за обучение.

Служителите трябва да бъдат обучени по уместен начин във връзка с гореспоменатото, преди да поемат задълженията си във връзка с идентифицирането, след което следва да се извършва редовно обучение поне веднъж годишно, както и когато възникне необходимост. Подобна необходимост ще е оправдана, ако например има промяна в правните и/или надзорни изисквания или в изискванията за защита на данните, които са в сила, в случай на съществен брой опити за измама, ако дадена институция научи за нови потенциални измами или ако процедурата има други недостатъци.

II. Встъпителна част

По време на процеса на идентификация служители трябва да се намират в отделно помещение с ограничен достъп.

III. Съгласие

В началото на видео идентификацията лицето за идентифициране трябва да даде изричното си съгласие с целия процес на идентификация, както и за това на лицето или неговия документ за самоличност да бъде направена снимка или моментна снимка.

Съгласието трябва да бъде въведено/записано недвусмислено.

IV. Технически и организационни изисквания

При задаване на случаи за идентификация на служителите трябва да има налични механизми за противодействие на предсказуемо разпределение на случаи и на свързаната с това възможност за манипулиране.

Видео идентификацията трябва да се извършва в реално време без прекъсване. Целостта и поверителността на аудиовизуалната комуникация между служителя и лицето за идентифициране трябва да е подходящо гарантирана, поради което се допускат само видео разговори с криптиране от край до край. Препоръките в Техническо ръководство TR-02102 на Федералната служба за сигурност на информацията (Bundesamt fur Sicherheit in der Informationstechnik - BSI) трябва да се спазват.

Освен това е необходимо подходящо качество на звука и картината по време на комуникацията, което да позволи недвусмислено и неограничено идентифициране въз основа на всички проверки, които се изискват в настоящата Циркулярна нота. Това включва в частност проверка на функциите за сигурност, категоризирани като подлежащи на визуална проверка в бяла светлина, както и извършената проверка за налични щети или манипулации на документа. За оценка на качеството на преноса на изображения трябва да са зададени подходящи информативни елементи на изображението като гилош модели и микро надписи.

При процеса на видео предаване съответният служител трябва да създаде снимки/моментни снимки, които ясно показват лицето за идентифициране, както и предната и задната страна на документа, използван от лицето за идентификация, и информацията, която се съдържа на този документ.

V. Допустими документи за самоличност

При процеса на видео идентификация като доказателство за самоличност съгласно всички наредби срещу изпирането на пари могат да се използват само документи за самоличност с функции за сигурност с достатъчна степен на защита от измама, които са ясни за идентифициране и следователно подлежат на визуална проверка както с бяла светлина, така и с наличната технология за пренос на изображения (можете да видите списъка в B.VI), както и които имат машинно четима зона.

VI. Проверка на документа за самоличност

За да установи самоличността на лицето за идентификация въз основа на допустимия документ за самоличност, служителят трябва първо да се увери, че документът, използван като доказателство за самоличност, съдържа оптичните функции за сигурност, идентифицируеми визуално на бяла светлина, които документите от този вид съдържат обикновено.

В зависимост от вида документ оптичните функции за сигурност включват:

Дифракционни характеристики:

- Холограми
- Идентиграма
- Кинематични структури

Технология за персонализиране:

- Наклонени лазерни изображения

• Типография

Материал:

• Отвор (например персонализиран)

• Защитна нишка (персонализирано)

• Оптично променливо мастило

Защитено отпечатване:

• Микронадписи

• Гильош модели

Съвпадение се приема, ако са спазени критериите за проверка на поне три от функциите за сигурност, избрани на случаен принцип от различни категории в гореизложения списък, за целите на идентифициране и приложени в документа за самоличност.

Служителят трябва също така да се увери, че документът, използван като доказателство за самоличност, съдържа другите официални характеристики, визуално идентифицируеми на бяла светлина и достъпни за проверка (включително оформление, номер, размери и разстояние между знаците, както и типография), които документите от този тип съдържат обикновено.

С употребата на подходящи IT програми трябва да се гарантира, че оптичните функции за сигурност, които се виждат на бяла светлина при видео идентификацията, съвпадат по форма и съдържание с отделните характеристики, които документът съдържа (например чрез сравняване на първичната и вторичната снимка като Идентиграмата, наклоненото лазерно изображение и др.) или че те съвпадат при справка с база данни за документи за самоличност.

Като алтернатива на използването на IT поддръжка подобно сравнение трябва да стане възможно с изображения, избрани от служителя (при възможност от сериен запис или от поредица записани видеоклипове) и въведени като задължителна част от процеса на идентификация.

Служителят също така трябва винаги да проверява дали документът за самоличност не е повреден, не е бил манипулиран и по-конкретно дали има поставена снимка.

По време на визуалната проверка лицето за идентифициране трябва да наклони документа си хоризонтално или вертикално пред камерата и да извърши всякакви допълнителни движения, които служителят може да поиска.

Структурата на интервюто с лицето за идентификация трябва да се променя поне по отношение на реда и/или вида на въпроси, задавани от служителя.

Срещу всяко заместване/манипулиране на части или елементи от документа за самоличност трябва да се предприемат съответни мерки. За тази цел лицето за идентифициране трябва да бъде помолено например да постави пръст върху части от документа за самоличност, свързани с елементи за сигурност (те са разнообразни и се избират от системата на случаен принцип), и да придвижи ръка пред лицето си.

Използвайки снимки от тези движения, които се изрязват и увеличават, служителят трябва да потвърди, че документът за самоличност и всички функции за сигурност, които подлежат на визуална проверка на бяла светлина, са напълно покрити в правилната точка, както и че в преходните точки не се наблюдават промени в резултат на човешка намеса, показващи манипулация.

Като част от процедурата за видео идентификация трябва да се извърши проверка на валидността и правдоподобността на данните и информацията, които се съдържат в документа за самоличност.

Наред с други неща това включва проверка на съответствието между датата на издаване и датата на изтичане на документа за самоличност. Датата на издаване в частност не трябва да е в бъдещето.

Освен това периодът на валидност на документа за самоличност не трябва да противоречи на нормите за документите за самоличност от този тип.

Друг необходим елемент от процеса на идентификация е автоматизирано изчисление на контролните цифри в машинно-четимата зона и кръстосаната проверка на предоставената там информация с информацията, която се вижда на документа за самоличност. Използваните ортография на цифрите, код на органите и шрифт трябва също да бъдат проверени, за да се гарантира верността им.

Лицето за идентификация също така трябва да сподели пълния сериен номер на документа за самоличност по време на видео предаването.

VII. Проверка на лицето, което трябва да бъде идентифицирано

Служителят трябва да се увери, че снимката и личното описание на документа за самоличност отговарят на лицето за идентифициране. Снимката, датата на издаване и датата на раждане трябва също да отговарят.

Използвайки психологически въпроси и наблюдения по време на процедурата за идентификация, служителят трябва да се увери в правдоподобността на информацията, която се съдържа в документа за самоличност, информацията, предоставена от лицето за идентифициране по време на интервюто, както и посоченото намерение на лицето. Могат също да се задават въпроси например по отношение на възрастта на лицето за потвърждение на снимката на документа за самоличност, както и датата и мястото на раждане, посочени в документа за самоличност. Лицето за идентифициране трябва да потвърди причината за идентификацията, най-малко за да е наясно лицето защо е необходима подобна процедура. Служителите трябва да са обучени как да определят без съмнение, че лицето за идентифициране закупува съответния продукт от избрания от тях доставчик (поради риск от фишинг, социално инженерство, действия под натиска на чужди лица и др.).

Служителят трябва също така да се увери, че всички данни на лицето за идентифициране съвпадат с данните, с които разполага задълженото лице и с които разполага служителят (когато е приложимо).

VIII. Прекратяване на процеса за видео идентификация

Ако описаната по-горе визуална проверка е невъзможна (например поради лошо осветление или лошо качество на видеото) и/или не е възможна вербална комуникация с лицето, процесът на идентификация следва да се прекрати. Същото важи и при други несъответствия или неясноти.

В подобни случаи може да се извърши идентификация по някой от останалите методи, позволени съгласно Закона за пране на пари.

IX. Предаване на TAN

По време на видео предаването лицето за идентификация трябва директно да въведе онлайн поредица номера (TAN), която е валидна само за тази цел и е компютърно генерирана и изпратена на лицето (чрез имейл или SMS) от служителя, след което трябва да върне TAN на служителя по електронен път. След като лицето за идентифициране въведе TAN, процедурата за идентификация приключва при успешното им потвърждение.

X. Запазване и записване

Всички отделни стъпки на целия процес на видео идентификация трябва да бъдат записани и запазени от задълженото лице или трета страна, на която задълженото лице е възложило процедурата за идентификация съгласно Раздел 7 (2) от Закона за прането на пари, или което задълженото лице е ангажирало съгласно Раздел 7 (1) от Закона за прането на пари по удостоверим начин за целите на вътрешен и външен одит и за BaFin. Поради тази причина изискването за документиране включва както визуален, така и звуков запис и запазване на цялата процедура, която трябва да е спомената в горепосоченото съгласие, дадено от лицето за идентифициране. Записите трябва да показват както това, че са изпълнени общите изисквания за идентификация съобразно законодателството срещу прането на пари, така и че са покрити минималните изисквания за видео идентификация, изложени в настоящата Циркулярна нота.

Записите трябва да се съхраняват в продължение на пет години съгласно Раздел 8 (3) от Закона за прането на пари

XI. Защита на данните

Искам изрично да подчертая, че горепосочените надзорни изисквания остават в сила независимо от всякакви други изисквания, които трябва да се изпълняват съгласно Раздели 7 и 8 от Закона за прането на пари, и без да се нарушават правата за защита на данните, които трябва да се спазват успоредно с това.

Настоящата Циркулярна нота влиза в сила на 15 юни 2017 г.

С настоящото отменям Циркулярна нота 4/2016 г. от 10 юни 2016 г., която първоначално бе отменена само временно.