Electronic Money Association
Crescent House
5 The Crescent
Surbiton
Surrey
KT6 4BN
United Kingdom
Telephone: +44 (0) 20 8399 2066
Facsimile: +44 (0) 870 762 5063
www.e-ma.org

Public Consultation Team,
Financial Action Task Force (FATF),
Paris, France

By email: FATF.Publicconsultation@fatf-gafi.org

29 November 2019

Dear Sir/Madam,

Re: Public consultation on FATF draft guidance on digital identity

The EMA is the EU trade body representing electronic money issuers and alternative payment service providers. Our members include leading payments and e-commerce businesses worldwide that provide online payments, card-based products, electronic vouchers and mobile payment instruments. The majority of our members operate throughout the EU, almost always on a cross-border basis. A list of current EMA members is provided at the end of this document.

Our members rely almost exclusively on remote know your customer (KYC) processes, and have done so for up to 20 years.

A key factor impacting customer take-up of new products is the practical means of undertaking customer due diligence (CDD), and in particular that of customer identification and verification of identity.

The challenges faced by members in relation to CDD and KYC include:

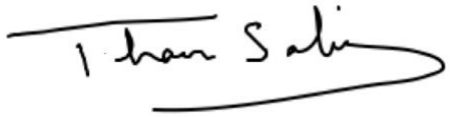
- Minimizing friction for account take up for new customers
- Finding an effective means for completion of CDD in a non-face to face environment; that is the availability of requisite data, or technology
- Implementing effective controls to mitigate the risk of identity theft
- Ensuring regulatory requirements allow for a range of CDD methods to be used, and not prescribing a single or narrow range of methods that may not be easily implemented or whose cost may be disproportionate to the product offering
- Recognising the contribution of indirect means of CDD such as those based on electronic footprint, data collected over a period of time, and customer behaviour

The EMA welcomes the FATF Guidance, as it will support the establishment of robust processes

for digital identification and ongoing monitoring processes which will support the fight against financial crime.

Thank you for your consideration.

Yours faithfully



Dr Thaer Sabri
Chief Executive Officer
Electronic Money Association

Areas of focus

1. **Are there any specific money laundering / terrorist financing risks, that arise from the use of digital identity systems for CDD, other than those already mentioned in Section IV of the guidance?**
   If so, how can they be addressed and by whom? Are there specific opportunities for combatting money laundering / terrorist financing that are not already mentioned in the guidance?

We concur with the benefits of digital ID systems set out at paragraph 107 to 112, including those of reliability, improved customer experience, decreasing the subjective nature of the process, allowing for better monitoring and increasing financial inclusion.

The potential risks must therefore be weighed against the benefits, whilst seeking to mitigate these where they occur.

Risks such as those related to the security of the channel, potential data breaches, lifecycle management of the ID credentials, impersonation fraud, privacy and infrastructural requirements as well as financial inclusion challenges, will all need to be address and mitigated as part of the deployment of digital ID infrastructure.

Given the dynamic nature of digital verification it is likely that risks and any potential mitigation measures will develop as the landscape progresses and greater use is made of it.

We note also that a number of risks identified in the paper are not unique to digital verification procedures, and would apply equally to traditional due diligence measures. In some instances, for example the risk of impersonation fraud, the use of several data points including biometric information, particularly where this is from an independent verifiable source, will mitigate this risk more effectively than traditional methods.

2. **What is the role of digital ID systems in ongoing due diligence or transaction monitoring?**
   a) What information do you capture under authentication at on-boarding and during authorisation for account access? Who captures this data?

Ongoing due diligence: will take place routinely, seeking to identify departures in behaviour from those of baseline expectations, or from those of comparator customers. Also seeking to confirm that data submitted at the outset continues to be up to date. In most cases, this is a self certification process.

Specific triggers for re-screening include the identification of changes to the profile of the customer account. For example, this might include changes in the volumes or values of transacted payments, the use over a period of time of different IP addresses to access the

system, or a different name or email addresses from those provided during account opening at the outset of the relationship.

Data captured: the type and volume of information captured will depend on the type of product, the risk that is assessed, and individual firms' policies and processes.

Information captured and recorded will in most cases include the following:

- Name
- Address
- Date and place of Birth
- Email address
- Internet Protocol (IP) Address and device footprint

Additional data that is captured by most of if not all PSPs will include a subset of the following:

- Mobile phone number and device footprint.
- Global Positioning System (GPS) location of device belonging to user
- Verified Government ID Card
- Passport including Photograph and number – potentially biometric information
- Driving Licence
- Utility Bill
- Source of Wealth (SOW) Information – Payslip, Business accounts and other documentation evidencing wealth.
- Source of Funds (SOF) Information – documentation supporting transaction source of funds

Furthermore, once checks are undertaken, the following information is recorded:

- Sanctions screening, and Politically Exposed Person (PEP) search results – false positive or true match
- Result of check against credit reference agency ID verification database
- Results of Internet searches
- Social Media Profile/Business profile – results

Approaches to digital verification processes: where ID verification is undertaken by reference against external databases (government databases, electoral roll, etc.) the PSP captures the data and then sends a query to the Authentication service provider through their Application Processing Interface (API). The response received will then result in verification with a calculated degree of confidence, or may require further proof of identity where the degree of confidence is insufficient or a match is not found.

Recording of data: the customer verification of identity information will be held either by the firm or a third party under an outsourcing agreement with the ID verification service provider.

Under this arrangement records will be retrievable without undue delay at any time, up to the statutory time limit for data storage required under local AML legislation.

b) Is the authentication data you capture relevant to ongoing anti-money laundering and counter terrorist financing due diligence and/or transaction monitoring? If yes, how?

The authentication data captured help the PSP to establish a base-line for ongoing monitoring (customer's geolocation, IP address, device footprints, behavioural biometrics etc.) and may also help flag departures from submitted data, such as address or country of residence etc.

Unusual activity can be flagged for investigation purposes, analysed, and where appropriate the account can be suspended or a Suspicious Activity Report made to the appropriate authority.

Transaction Monitoring:

Fraud scenarios: where the customer has initiated a transaction, which given its context, and contextual data collected, raises suspicions of fraud, push notifications on the mobile phone device can alert the customer in real time. The customer can then either confirm the transaction is correct or raise concerns, resulting in a fraud investigation within the firm. This can be combined with suspension of transactions or requirements for additional authentication.

Anti-money laundering (AML) – contextual data can help trigger systems that are programmed to look for individual flags, or for patterns of behaviour that are informed by AML typologies. Once identified, investigation, suspension and/or reporting can be undertaken.

Terrorist Financing (TF) – similarly, contextual data in relation to geographic location, merchandise purchased, country information can inform monitoring systems that are intended to identify patterns based on known typologies. Appropriate reporting can then be undertaken and action taken.

3. **How can digital ID systems support financial inclusion?**

a. **How can digital ID systems with different assurance levels for identity proofing/enrolment and/or authentication be used to implement tiered CDD, allowing clients a range of account functionalities depending on the extent of CDD performed, and particularly in situations of lower risk? Please provide any practical examples.**

Financial exclusion can be caused by a range of factors, from the absence of traditional means of identity documents (e.g. students or under-18) to an absence of online financial data (e.g. cash reliant economies), or an absence of electronic or economic infrastructure in the relevant jurisdiction (e.g. developing economies). Other factors set out at paragraph 138 that are specific to certain demographies or populations are also relevant.

Supporting financial inclusion will therefore vary with the circumstances; in some instances it provides a shortcut bypassing the need for physical documentation, it may provide an alternative to conventional CDD credentials where the risk is low –(for example allowing for the collection of alternative or a subset of identity credentials), and could over time provide a means of monitoring and assessing risk based on detected data and transaction data. This could in turn mitigate any risk posed by the use of non conventional credentials.

Provided that technology is appropriate to the circumstances of user, (cost is accessible, infrastructure is in place, know-how is present) it could provide a means of accessing a wider range of financial services, if a device can play a role in the identity verification and subsequent authentication processes. This would include mitigation measures that would result from monitoring transactions and detection and use of data.

It should be noted however, that this is almost entirely dependent on the local regulatory framework allowing for such an approach to CDD, for the regulator being confident in the robustness of such an approach, and in the FATF mutual evaluators recognising such approaches as robust and valid.

Tiered approach to CDD: the ability to implement different levels of CDD are key to (i) the offering of different payment services of varying functionality, and (ii) the staged offering of different functionalities on a single product, enabling financial inclusion. An example might be the restriction of the use of a payment product so that a low value can be transacted, or cash withdrawn, either until additional data has been provided, or until historical data supports and compensates for such information. This progressive approach allows the customer to access financial services, whilst at the same time the firm is able to establish a relationship and mitigate any risks in real time.

Even where customers may not be able to produce sufficient ID documentation for verification purposes (e.g. Passport/Driving Licence/ID Card) they may have a sizeable digital footprint that allows PSPs to verify identity in low risk situations.

It should also be noted that more detailed or elaborate CDD may be inappropriate for certain products that have a limited functionality and are of limited value to the user. The user may think the provision of detailed identity information is not warranted by a payment product that issued for and used within a limited environment. Additionally, the cost of such CDD may outweigh the revenue generated by limited purpose products.

Conversely, access to online information about a customer, sourced from multiple providers as well as publicly available data may enable enhanced due diligence to be undertaken on a customer in a rigorous manner, perhaps exceeding that of conventionally obtained EDD data.

b. **Have you adopted lower assurance levels for identity proofing to support financial inclusion? What additional measures do you apply to mitigate risks? Please provide any practical examples.**

Simplified Due Diligence (SDD) – product offerings can be adopted where due diligence is delayed at onboarding, but capped limits apply. Once these limits are reached, further due diligence takes place. These products encourage financial inclusion and are often used by migrant workers and other vulnerable customer groups who may not fulfil traditional due diligence requirements and otherwise be unable to access financial services.

c. **How can progressive CDD via digital ID systems aid financial inclusion (i.e. establishing greater confidence in a customer's identity over time)?**

Progressive CDD – in this scenario a basic verification is conducted at the outset of customer relationship. This is then followed by detailed Transaction Monitoring and ongoing monitoring using data points – GPS – location, spending and loading, as well as behavioural biometrics.

In these circumstances due diligence is conducted using a risk-based approach and the due diligence measures applied are commensurate with the level of risk the customer poses.

4. Does the use of digital ID systems for CDD raise distinct issues for implementing the FATF record-keeping requirements?

a. What records do you keep when you use digital ID systems for CDD?

Different types of ID verification services generate different records:

- Video ID
- Biometric identification
- Collected data sent to outsourced ID verification service providers, data checked against datasets that are held or can be accessed by these providers, results for each checked returned (Match Y/N, confidence interval score), etc.
- In-house checks completed

Data collected during this process will either be stored on PSP systems or in the systems managed by an outsourced service provider; data will be accessed by the PSP Customer Service function/Anti-money laundering (AML) function and Fraud management team.

The ability to ensure that records are kept for the contracted period that their integrity and authenticity is protected and that they will continue to be accessible is a key objective. This is an important focus for firms adopting solutions offered by third party providers. Usage scenarios that involve sharing customer data collected during the on-boarding process with 3rd party providers are complicated by the data privacy requirements introduced by the EU General data protection regulation (GDPR) especially when customer data are shared with 3rd party CDD verification service providers whose systems are based outside the EU

b. What are the challenges in meeting record-keeping requirements when you use digital ID systems for CDD?

The use of digital tools for verification, screening and ongoing monitoring does not - on its own - raise specific problems in terms of the record keeping obligations provided that records are stored within the firm or are readily accessible.

c. If you keep different records when using digital ID systems for on-boarding, does this impact other anti-money laundering and counter-terrorist financing measures (for example ongoing due diligence or transaction monitoring)?

The use of digital tools for verification and screening during customer onboarding does not have a detrimental impact on other AML or Counter Terrorist Financing (CTF) measures such as transaction monitoring or ongoing customer due diligence.

The use of such tools does introduce a requirement to exchange such data in a secure manner across authorised applications/parties that may use them to complete activities such as AML/CTF enforcement. Note the comment raised under 4a above of the GDPR compliance requirements introduced by the transfer of onboarding records with 3rd parties or beyond EU borders

List of EMA members as of November 2019:

AAVE LIMITED
Airbnb Inc
Airwallex (UK) Limited
Allegro Group
American Express
Azimo Limited
Bitstamp
BlaBla Connect UK Ltd
Blackhawk Network Ltd
Boku Inc
CashFlows
Circle
Citadel Commerce UK Ltd
Coinbase
Contis
Corner Banca SA
Curve
eBay Sarl
ePayments Systems Limited
Euronet Worldwide Inc
Facebook Payments International Ltd
First Rate Exchange Services
Flex-e-card
Flywire
GoCardless Ltd
Google Payment Ltd
IDT Financial Services Limited
Imagor SA
Intuit Inc.
Ixaris Systems Ltd
Moneyhub Financial Technology Ltd
MuchBetter
myPOS Europe Limited
Nvayo Limited
One Money Mail Ltd
OpenPayd
Optal
Own.Solutions
Park Card Services Limited
Paybase Limited
Paydoo Payments UAB
Payoneer
PayPal Europe Ltd
Paysafe Group
PPRO Financial Ltd
PrePay Solutions
QIX Ltd
Remitly
Revolut
SafeCharge UK Limited
Securiclick Limited
Skrill Limited
Soldo Financial Services Ireland DAC
Stripe
SumUp Limited
Syspay Ltd
Transact Payments Limited
Transact24 (UK) Ltd
TransferMate Global Payments
TransferWise Ltd
TrueLayer Limited
Trustly Group AB
Uber BV
Valitor
Vitesse PSP Ltd
Viva Payments SA
Wirecard AG
Wirex Limited
WorldFirst
Worldpay UK Limited