Know your Customer:
Retail customer verification in the Single Market

July 2018
The digital transformation is one of the key challenges today – also for the financial industry. The Association of German Banks is meeting this challenge by, among other things, cooperating with start-ups from the financial sector, fintechs. The cooperation was institutionalised in the Digital Banking Project Committee, which is vigorously driving forward the cross-cutting issue of digitisation. The committee is a high-level body comprising bank Chief Digital Officers (CDOs) and leading figures from the German fintech scene. The present paper is the result of intensive cooperation between banks and fintechs.

Common positions of banks and fintechs

The digital transformation is one of the key challenges today – also for the financial industry. The Association of German Banks is meeting this challenge by, among other things, cooperating with start-ups from the financial sector, fintechs. The cooperation was institutionalised in the Digital Banking Project Committee, which is vigorously driving forward the cross-cutting issue of digitisation. The committee is a high-level body comprising bank Chief Digital Officers (CDOs) and leading figures from the German fintech scene. The present paper is the result of intensive cooperation between banks and fintechs.

Contacts at the Association of German Banks:
Tobias Frey | Legal Affairs | tobias.frey@bdb.de
Mario Labes | Fiscal Affairs | mario.labes@bdb.de
Tobias Tenner | Digital Banking | tobias.tenner@bdb.de
Preamble

The financial services sector is undergoing a radical transformation affecting retail business in particular. New companies, so-called ‘fintechs’, have entered the market with new business models and new products. The Association of German Banks (BdB) is responding to this transformation: it supports cooperation between banks and fintechs and is instrumental in ensuring that common positions can be found.

A feature of many banks and fintechs is that they operate across national borders. This, in turn, poses specific challenges: in the face of digitisation, cross-border companies are increasingly addressing the question of the extent to which processes can be performed uniformly and centrally for the entire company from one EU member state, taking account of national legislation in each case. The primary focus here is on the so-called ‘know your customer’ (KYC) processes. KYC processes mean the collection and verification of data required by law. Of particular importance in this context are EU member states’ anti-money laundering laws, but also tax regulations, e.g. the Fiscal Code in Germany, as well as other provisions that are either purely national or reflect EU law.

KYC processes are a key aspect for all companies operating in the financial marketplace with customer data. Yet different arrangements in EU member states hinder cross-border digital approaches to customer acceptance by entities obliged to comply with KYC requirements (‘obliged entities’).

The European Commission shares this view: it noted in its December 2015 Green Paper on retail financial services that the differences between legislation in force in member states seriously affect the costs and risks associated with cross-border retail financial services.

Differing requirements for verification and reusability of the data collected are particularly to blame for the fact that in most cases KYC processes cannot be used or reused digitally or across borders within the EU. Whenever they enter into a business relationship with an obliged entity (both across borders and within an EU member state), customers and consumers are usually forced to undergo the KYC process all over again. This is inconvenient for them, impedes cross-border use of financial products and undermines efforts to achieve increasingly digital, efficient and user-friendly cross-border e-governance. What is more, it leads to gaps in consumer protection since, for customers, switching banks within their home country or entering into a business relationship outside their home country is needlessly made more difficult. And this despite the fact that the Payment Accounts Directive (2014/92/EU) was actually intended to strengthen consumer protection and to facilitate and encourage switching banks within the home country and establishing a business relationship outside the home country.

The Second Payment Services Directive (‘PSD2’) (EU 2015/2366) has the same thrust. Though this directive essentially deals with cross-border and secure payment services, the functions it addresses (e.g. access to bank interfaces) would be likely to support the digital Single Market through the transfer of data and thus allow the reuse of data on behalf of customers.

The requirement to perform reverification in every case without being able to reuse an initial verification increases the administrative burden on obliged entities and consumers alike. The basic need for innovative KYC process solutions at European level is, in fact, acknowledged. This is underlined, for example, by the ‘Opinion on the use of innovative solutions by credit and financial institutions in the customer due diligence process’, published by the European Supervisory Authorities (ESAs) on 23 January 2018. The ESAs’ right approach does not go far enough, though. Particularly the reusability of KYC processes is not yet on the ESAs’ agenda. Progressing the right approach towards the reusability of initial verification is, however, equally important in
In this position paper, drafted jointly by banks and fintechs, the Association of German Banks wishes to draw attention to the existing challenges and propose regulatory solutions.

**Collection of data**

Private banks and fintechs would like to see the KYC data to be collected defined uniformly and exhaustively EU-wide for all products. Every natural person resident in the EU should be assigned a unique identification feature (e.g. identification number or a certificate).

This EU identification feature should replace all current identification numbers (national number in Belgium, Tax Identification Number (TIN) in Germany, numbers on passports and identity cards, etc.).

**Needed: convenient, innovative and uniform KYC processes for the Single Market**

**This requires:**

- uniformly defining the KYC data to be collected,
- standardising the identity documents to be uniformly admissible for verification, including security features,
- defining a uniform EU-wide identification feature (number or certificate) and, at the same time,
- remaining open to new verification procedures through automatic ‘most favourable treatment’ of procedures that are admissible and thus regarded as sufficiently secure in an EU member state and
- permitting the reuse of KYC processes, performed in accordance with EU legal standards, on the basis of uniform criteria.

order to further strengthen both the EU as a business location in international competition and pan-European consumer protection.
Verification of data

In line with the principle of ‘most favourable treatment’, verification procedures admitted in one EU member state must automatically be admissible across the EU. The Commission should publicly hold and maintain a list of the verification processes admitted in member states, including the necessary process-related requirements in each case, to allow application of the ‘most favourable treatment’ principle when verification processes are admitted in practice. At the same time, standardisation not only of European passports but also of identity cards and driving licences would be helpful. This would also have to include their security features and their endowment with the required human and machine-readable EU identification feature.

Reusability

The reuse of initial customer verifications performed in accordance with EU legal standards should be allowed for further verifications elsewhere across the EU. In this case, the party performing the initial verification would be tasked with recording and transferring the data correctly. Adopting an initial verification instead of requiring a new verification from the customer should be a risk-based decision by the obliged entity, so that – taking into account how old the initial verification is, for example – it can choose between reuse and reverification. Nothing would therefore change as regards how responsibility for the KYC check is distributed. A bank that establishes a new business relationship is already solely responsible today for performance of the KYC process. That goes even if a third party recognised as trustworthy per se or by contract is included in the KYC process.

Explanation of the underlying problems and requirements

Collection of data

In the EU member states, different KYC data are collected, though not all European consumers automatically have these at their disposal. Apart from this, the data to be collected differ not only from one member state to the next but also with regard to the product (e.g. current account or custody account) for which verification is performed.

The lack of harmonisation and the accompanying uncertainty for business models hamper innovation in the EU, particularly within the financial sector. They thus also affect the ability to compete with international providers.

The criteria for identifying a low, simple, or high risk of a particular customer laundering money or financing terrorism are also defined differently within the EU, though these determine, among other things, the amount of data to be collected. Broadly adopting a risk-based approach without providing enough sufficiently concrete examples at European level leads to a complete fragmentation of the Single Market. With
data minimisation in mind, only data that can actually be requested from the customer/consumer and verified should have to be collected. Which customer/consumer data must be collected should, however, be regulated uniformly and exhaustively EU-wide in a non-risk-based manner by means of a minimum data record on the customer/consumer as a natural person.

A host of different, mostly nationally designed identification numbers are currently in use across the EU, and these often have to be recorded under country-specific KYC processes when an account is opened. Examples are the Tax Identification Number (TIN) in Germany, Documento Nacional de Identidad (DNI) in Spain or National Insurance Number (NIN) in the UK. The introduction of a uniform EU-wide identification feature (number or certificate) for every EU citizen would be advisable here. In the process, it must be ensured that every EU citizen is actually assigned only one specific EU identification feature. Representatives of obliged entities should be involved in definition of this EU identification feature, with any existing conventions being used as a basis.

A uniform EU identification feature would also be important for the interconnection of account data retrieval systems and central account registers in the EU member states. This is of particular importance as the Fifth Anti-Money-Laundering Directive now requires the introduction of account data retrieval systems/central account registers and their interconnection. The direct cross-border access of national EU law enforcement agencies to data retrieval systems/central account registers in other EU Member States, envisaged by a European Commission proposal for a Directive, can, moreover, only make sense if uniform data records respecting the principle of data minimisation and the right of ‘informational self-determination’ are available there. This is not, at any rate, the case when it comes

---

**Examples**

- In some cases, a residential address has to be recorded, in other cases a postal address or a personal address. Particularly bearing in mind that natural persons, particularly free-lancers, may well have not only a residential address but also a business address, this is problematic.

- There are no uniform and exhaustive rules for recording the different parts of a name, e.g. several first names, nobiliary particles (sometimes transformed to simply being part of the name), academic degrees or titles.

- In Germany, the German Tax Identification Number (TIN) always has to be recorded where the consumer/customer possesses one (Section 154 of the German Fiscal Code). Apart from discrimination of German residents, it appears that in this case – because of the need to check whether no German TIN is actually available – the German arrangement may even discriminate indirectly against citizens of other EU member states.

- For verification in the case of a cashless transaction not exceeding EUR 1,000, other data have to be recorded under the EU Funds Transfer Regulation than for verification under the German Anti-Money Laundering Act where cashless transactions exceeding EUR 1,000 are involved.
to the German Tax Identification Number (TIN) stored under the German account data retrieval system.

Uniform KYC processes across the EU are also necessary particularly from the perspective of consumers to allow them to enter into a cross-border business relationship with an obliged entity without any in-depth knowledge of the respective national regulatory requirements.

**Verification of data**

The ‘passportability’ of verification processes, i.e. their cross-border, EU-wide use in the Single Market, is only possible to a very limited extent.

Not only the EU member state identity documents admissible for verification, but also the security features of such identity documents, vary from one member state to the next.

Which data have to be verified and to what extent is something that is not regulated uniformly either.

For verification of customers/consumers by obliged entities, member states rely on admission of national solutions that ultimately lead to a wide range of different processes. The problem is that this essentially welcome innovative diversity remains confined in each case to national borders. An innovative KYC process admitted in one EU member state is not automatically recognised in all other member states.

The absence of any automatic ‘most favourable treatment’ impedes the proliferation of convenient, innovative KYC processes, such as video identification, for example. Particularly such KYC processes are, however, of great importance for the digitisation of the Single Market and also deliver significant added value when it comes to effectively combating money laundering and terrorist financing. The latter was also acknowledged recently by the ESAs (see Preamble).

The approach providing for admission of uniform KYC processes via notification to the European Commission under eIDAS must be welcomed as a first step in the right direction. Yet this step is by no means sufficient to create a real level playing field and strengthen consumer protection. A point of criticism: at present, only EU member states can notify KYC processes to the Commission. Private undertakings cannot do so. There is no plausible reason to exclude processes developed by private undertakings from such notification.

The best way to foster innovation in KYC processes is to continue allowing national recognition of new KYC processes and to stipulate that KYC processes recognised in one EU member state are automatically applicable EU-

---

**Examples**

**Driving licence**

Under the German Anti-Money Laundering Act, German driving licences cannot be used to identify persons, as they do not meet passport and identity document requirements. In Austria, on the other hand, identification for anti-money laundering purposes is possible using an Austrian driving licence, as this is an admissible photo ID for such purposes. Identification for anti-money laundering purposes based on a driving licence is allowed in the UK as well.
wide, in line with the ‘most favourable treatment’ principle. Should this result in similar KYC processes, e.g. two KYC processes for verification by video chat, being admitted in different countries, the better solution will ultimately prevail, as both processes would be applicable across the EU. However, given the continuous dialogue that national supervisors conduct with each other and with the ESAs, virtually simultaneous admission of highly similar KYC processes in several EU member states is most unlikely. The application of the ‘most favourable treatment’ principle would therefore allow controlled competition between innovative verification processes in the EU and thus at the same time strengthen the EU as a digital financial marketplace.

Examples

**Valid identity document containing a different address due to a change of address**

What is the procedure if, possibly following a change of address (at short notice), a valid identity document contains an address that differs from the address provided by the customer/consumer?

There is as yet no uniform and exhaustive EU-wide arrangement for dealing with such cases. However, as flexible an approach as possible should be possible to allow risk-based reuse of initial verifications EU-wide. The ‘freedom of movement’ principle and a strong Single Market would be best served by such an approach.

**Video identification**

Video identification was first admitted in Germany, where it subsequently proved successful, particularly also in cross-border use. Especially customers from Austria opened accounts in Germany using the new video identification procedure, since this was often much more convenient for them than opening an account at a branch of an Austrian bank. Not only in Austria but also in other EU member states, this was seen as putting domestic banks and other obliged entities at a competitive disadvantage.

Consequence: Austria, Luxembourg, Spain, Portugal and further EU member states have since admitted the German-type KYC video identification procedure, adapted to their own national requirements and featuring in some cases different criteria. In other EU member states, including France and Poland, national admission of video identification is planned.

What is basically a success story also has a downside, however, since ‘the wheel’ is ultimately being reinvented in 28 EU member states for the KYC video identification process. Every member state sets different wheel sizes and different spoke lengths, so that providers remain confined to their national market or have to tailor their KYC process product separately to each member state. It goes without saying that this causes further problems for reuse of these KYC processes.
The solution would be automatic recognition by national supervisors of an admitted KYC process in all EU member states. In this way, Austrian banks would also have been able to simultaneously admit the video identification process without any distortion of the market in favour of German banks. Automatic recognition would preserve and foster the uniformity of the Single Market. The security of the new KYC process would be guaranteed through admission by national supervisors and customers/consumers would directly benefit from use of the new, convenient and innovative KYC process.

Reusability

There are no uniform EU-wide rules on whether – and, if so, under what conditions – KYC processes can be reused within EU member states or even across borders. Nor are there any uniform rules on the extent to which third parties may use completed KYC processes. This is true even where the verified customer consents to transfer of the KYC process.

Where reuse is permitted at least at national level, this is ensured partly by way of a legislative act, partly by way of an administrative order, yet always only in the respective EU member state on the basis of its own criteria for the KYC initial identification process. Cross-border reuse of KYC processes within the EU is therefore currently only possible to a limited extent and requires considerable time and effort. National law undermines the goal of a single, consumer-friendly European market in this respect.

Given the more or less chaotically differing national requirements, it is therefore virtually impossible to establish uniform processes for the transfer and reusability of verifications within a group or to/by third parties (e.g. public bodies). There can be no question of a level playing field and thus a Single Market as far as the reusability of KYC processes is concerned.

What needs to be done? Uniform admission of reusability would further drive forward the digital transformation of providers and create scope for actual use of e-governance offerings by EU citizens. It could dismantle significant barriers in the Single Market and would enhance the EU’s global competitiveness.

Uniform admission of reusability would also serve consumer protection. It would make switching a bank account within the home country or entering into a business relationship outside the home country even easier. This is in line with the EU’s declared aims. As explained, the provisions of the Payment Services Directive on help with switching an account (across borders) are already clearly aimed at encouraging and facilitating a change of banks by consumers. Yet these provisions fall short, as they fail to remove all the barriers that a consumer faces when changing banks. For customers, reusability would dismantle significant barriers and obstacles to the ‘freedom of movement’ principle, while generally improving the convenience of offerings by obliged entities. At the same time, it would make data repositories, as well as the history and transfer of data, more transparent.

In the interests of both consumers, obliged entities and public bodies, but also to realise a Single Market, harmonised, EU-wide rules on the reusability of a KYC process performed in accordance with the requirements of European law are therefore urgently needed. With the full harmonisation required on this point in mind, such
rules could be introduced by way of an EU Regulation. Such an EU Regulation would be effective if it were based on PSD2 and gave third-party providers access to customer accounts. It is, for example, conceivable that the verification data could be stored for the customer at the bank in a cloud. The customer could then allow third-party access to the data and documents on the basis of an appropriate contractual agreement. This approach should cover all verification processes that are admitted by supervisors of at least one EU member state. The decision on actual use of a process, also taking into account how old initial verification is, should be made by the obliged entity on a risk basis. The obliged entity already bears responsibility for this today. So there would be no change to this basic principle.

The reuse of KYC processes (catchword: ‘digital identity’) is not likely to be confined only to reuse within the financial sector. Reuse in the insurance, retail or administrative sectors would also be conceivable. In addition, it will create the basis for new business models (e.g. ‘IdentityHub’).

The reuse of data that can be enhanced by information such as the length of the customer relationship or the communication flow between customer and bank would be more meaningful than mere reverification based on an identity document. Not only the financial industry but also online merchants, who are facing an increase in identity theft or phantom (i.e. fake) identities, would benefit. And consumers would be protected against identity theft. Pro-active reuse of data would, moreover, ensure that that these are regularly updated.

The reuse of data also creates scope for creating innovative, convenient, barrier-free, secure cross-border KYC processes in real time. For example, it would be possible to handle an online order using a bank’s access data: the required data would be handed over and

---

**Examples**

**Regulation of reuse of KYC processes is highly fragmented in EU member states:**

In some EU member states, the (standard) transfer of a KYC process requires consent or at least notification to supervisors (in most cases, data protection supervisors). This is, for example, the case in Austria and France (mandatory consent) or in Luxembourg and Italy (mandatory notification).

In some cases, there are specific requirements regarding how old certain KYC documents are allowed to be: in Austria, they should not be older than six months; in Slovakia, not older than three months. In Luxembourg, there is the vague requirement that the KYC process has to be ‘up-to-date’.

In some countries, national requirements stipulate that foreign ID documents have to be translated into the local language by a certified translator and presented along with the original.

Finally, in some EU member states use of a KYC process performed by another bank is only permissible for anti-money laundering purposes. Other purposes, such as a lean and customer-friendly customer acceptance process, are not allowed; this applies in France, for example. In some cases, the KYC process is completely ruled out where enhanced due diligence requirements apply or only possible if further checks are performed, e.g. like in Austria or Slovakia.
immediately processed digitally. Customers could save themselves the trouble of entering data and undergoing the verification process and would have full control over who hands over which data to whom. Security could, for example, be ensured by means of two-factor authentication (2FA).

We can therefore draw the following conclusion: because of the associated effects, such as minimising costs and increasing efficiency, all parties would benefit from uniform EU-wide admission of the reuse of KYC processes.
The Association of German Banks can be contacted

by post:
Bundesverband deutscher Banken
P.O. Box 040307,
10062 Berlin
Germany

by phone:
+49 30 1663-0

by email:
bankenverband@bdb.de

online:
bankenverband.de