Stop losing customers to outdated KYC processes

Social KYC can help you reach more new users safely and cost-effectively.

A white paper from

veridu

RAMPARTS
European Law Firm

Whether you're regulated or not, it makes good business sense to know your customer, but there's a fine line between getting the information you need to do this and losing a potential user who feels your sign up process is unnecessarily difficult or infringes on their privacy. With billions of people all over the world using social media there are many good reasons to implement Social KYC as an alternative, or as a complement, to traditional methods of identifying users.

Background

The current form of Know Your Customer (KYC) regulation, introduced over a decade ago, was initially focused on banks, and as a result can feel like a hindrance to smaller and more nimble businesses, like cryptocurrency wallets and cross-border e-commerce companies.

Identity verification (IDV) is a particularly challenging aspect of the KYC process, and the traditional way of verifying identities using passports, driving licences and other documentary forms of identification is becoming a barrier. A barrier to trade, but judging by the increase in cases of identity theft (31% increase in the number of victims of identity theft in the UK alone[1]), not a barrier to criminals.

As if this wasn't enough, traditional identity verification mechanisms also have an unintended negative impact on financial inclusion. Users in developing countries and those under the age of 24 are often seeing themselves declined through no fault of their own simply because they don't have official identity documents or a comprehensive credit history.

This paper offers some ideas about identity verification in an online world. It explores some common challenges when using traditional methods, and will introduce a new approach — social KYC, using a person's digital footprint and online social identities to instantly verify and authenticate their identity with a high degree of confidence. This approach can also be used to reduce fraud and to manage compliance requirements as a complementary approach with other forms of KYC and IDV as required.

[1] Source: https://www.cifas.org.uk/id_fraud_first_quarter

A brief history

The current form of Know Your Customer (KYC) regulation, introduced swiftly after the 9/11 attacks in the United States, exists to prevent identity theft, financial fraud, money laundering, terrorist financing and other financial crimes. When the current regulations first came into force they were aimed predominantly at banks, but have now been extended to cover more sectors, including providers of cryptocurrency wallets in certain jurisdictions (recently the European Commission advised that all European cryptocurrency exchanges will become obliged entities under the 4th Anti-Money Laundering Directive[2]).

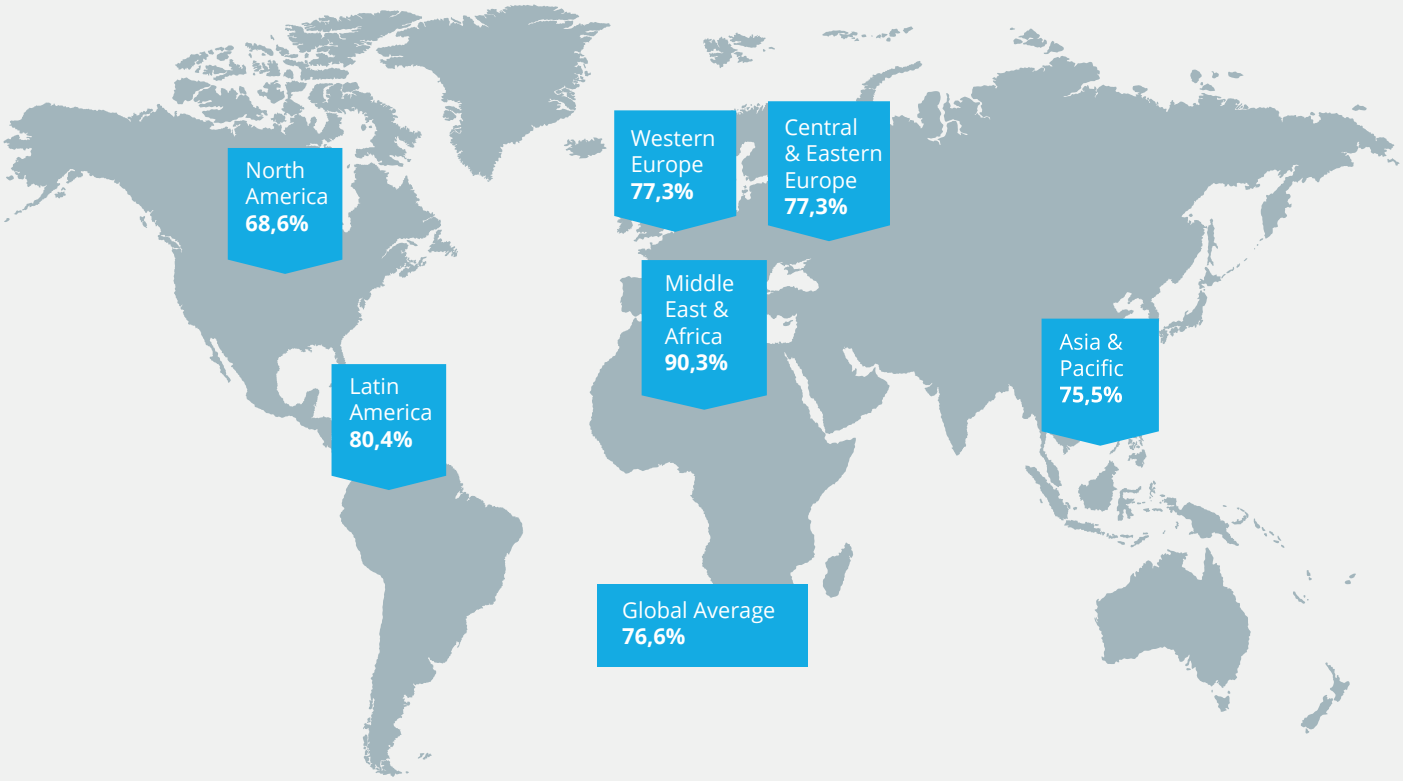
Regulation has also become more stringent but less prescriptive — less about ticking boxes and more about focusing your finite resources on the actual risks you face using a risk-based evidentiary approach. This push for firms to take a risk-based approach is a good thing — it gives you leeway to tailor your processes to meet the needs of your business whilst combating money laundering and terrorist financing.

Verifying the identity of a new customer is one step in the KYC process, and has traditionally been accomplished by checking a person's official identity documents. All well and good a decade ago when opening a bank account involved turning up at your local branch, completing paper forms and waiting patiently while all the relevant checks were carried out.

However, the environment companies operate in today is changing rapidly. We expect to be able to sign up to new services online, and often on the go, and we expect instant access. If we don't get it we'll go somewhere else, it's that simple.

This is where the risk-based approach, and the use of Social KYC comes in.

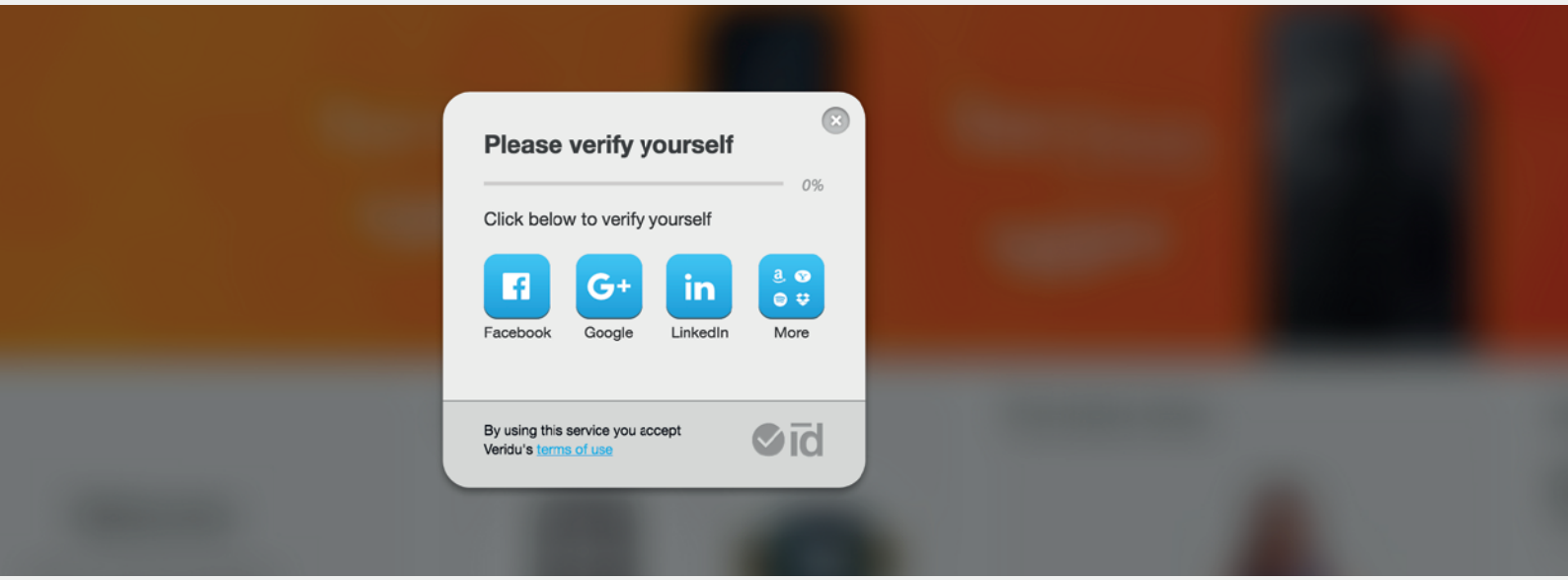
Social network user penetration worldwide
— Projection for 2016 (eMarketer April 2013)



[2] See EC Action Plan, 02 Feb 2016: *http://europa.eu/rapid/press-release_MEMO-16-209_en.htm*

What is Social KYC?

We generate large amounts of data about ourselves online every single day. We buy online, keep in touch with friends and family online, share photos, stream music and films, it goes on. All of this activity, when analysed as a whole, builds up a very deep and unique digital footprint — something that's exceedingly difficult for someone to steal or fake convincingly.



Social KYC harnesses this data and uses it to establish a person's identity — on a consent driven basis, of course. Using algorithms to analyse and corroborate various data attributes across multiple online accounts it is possible to quickly establish the likelihood of a person being:

- real
- who they claim to be (including various demographic data related thereto)
- a legitimate potential user (rather than a fraudster trying to access your platform with malicious intent)

We're all used to Single Sign On - using an existing social media account to sign up to a new service — and Social KYC is an extension of this. As all you're doing is asking a user to log in to a variety of their online accounts to prove who they are, it makes for a far more fluid sign up experience which in turn will encourage more users onto your platform.

KYC challenges

Today's KYC regulation was not developed with an electronic world in mind nor does it fully take account of emerging technologies, like cryptocurrency. KYC requirements can seem at odds with your needs when trying satisfy increasingly demanding consumers with sub-second response times and instant, low-cost global transactions. In addition, the latitude to rely on data instead of documents is currently enshrined in European law but many banks and regulators still insist on replicating the paper based IDV and KYC processes of the old world.

Three of the most common challenges facing the online industry are:

1. Sign-up friction

Long forms, credit reference checks, and sharing official identity documents — they all take time and add friction to your sign up process, not to mention increasing your overheads on each transaction.

If document collection and checks are part of your main onboarding process you need to be asking yourself why. Adding a 'physical' step into an otherwise purely online experience has a tremendously negative impact on user experience, an unnecessary evil in a world where online data about individuals is abundant. However, many may find it useful to request documents if primary checks have not provided sufficient verification or if any high risk factors are present that suggest further checks would be prudent, e.g. high risk of money laundering or a PEP (Politically Exposed Person) or sanctions list match.

2. Lack of official documents

The rise of the new middle class in emerging markets is a huge opportunity for cryptocurrency wallet providers. Many of these individuals are struggling to access traditional financial services because they don't have a credit history, official identity documents (e.g. passport or driving licence), or live in countries without government mandated identity cards or electronic identity programmes. This lack of documentation also affects young people.

If your KYC process relies only on document checks, what opportunities are you leaving on the table?

Conversely, if you've made the decision not to do any KYC at all because of the difficulty in verifying identity in the markets you operate in, what risks are you exposing your business to?

3. Cost

Traditional forms of verifying identity can be expensive. It takes people to gather and review physical documents, and credit reference agency checks aren't cheap.

Harnessing online data, on a consent-driven basis, is a reliable, yet highly cost-effective alternative to this challenge.

These challenges really only exist if you simply choose to follow the crowd when it comes to developing your KYC processes. Why look to the big banks for inspiration? They've had years to develop and refine processes that were built for a world that has changed. Many have thrown substantial amounts of money and people at the problem to compensate for outdated technology, and are still coming under fire from regulators for not getting it right.

Emerging technology companies have the ability to start from scratch to build processes that completely fit in with their business requirements and that put the customers' requirements of speed and ease first. Getting it right requires that you use efficient and proportionate processes to risk management and that you are able to explain those decisions and processes to your regulators and board.

Identity and how to prove it

So do you really need to see those documents?

The EU Anti-Money Laundering Directive (Directive) states that customer's identity can be verified using documents, data or information.

> *Customer due diligence measures shall comprise:*
>
> *"identifying the customer and verifying the customer's identity on the basis of documents, data or information obtained from a reliable and independent source"*
>
> (Article 13, 4th Anti-Money Laundering Directive)

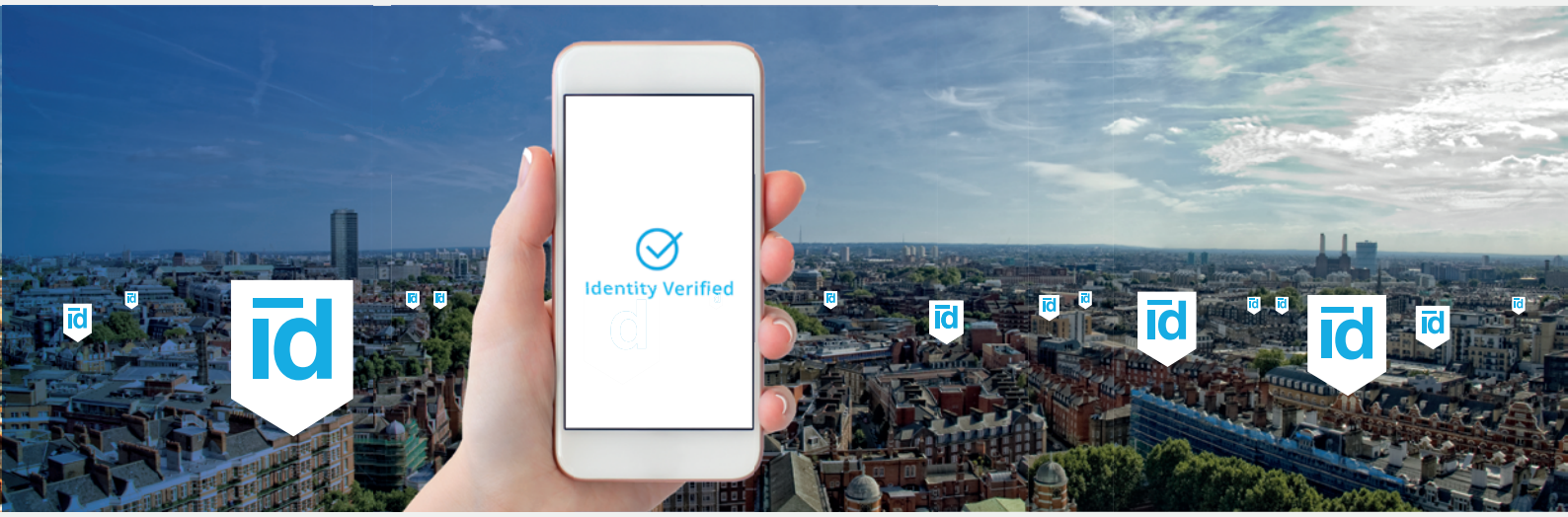
The UK Joint Money Laundering Steering Group (JMLSG) guidance (UK Guidance) offers cross-sector guidance and they emphasise your responsibility to make your own judgements based on the information available and using a risk-based approach.

> *"Evidence of identity can take a number of forms. In respect of individuals, much weight is placed on so-called 'identity documents', such as passports and photocard driving licences, and these are often the easiest way of being reasonably satisfied as to someone's identity. It is, however, possible to be reasonably satisfied as to a customer's identity based on other forms of confirmation...*
>
> *... How much identity information or evidence to ask for, and what to verify, in order to be reasonably satisfied as to a customer's identity, are matters for the judgement of the firm, which must be exercised on a risk-based approach..."*
>
> (JMLSG Guidance 5.3.28 and 5.3.29)

The Directive also allows for firms to carry out simplified due diligence (SDD), as part of a risk based approach, if certain conditions are met, e.g. depending on the person concerned or the product involved. SDD means that firms do not have to carry out full customer due diligence but it does not normally equate to fully anonymous transactions either, operators should ensure they can explain and justify situations where SDD is appropriate.

The UK Guidance states that identity would typically include full name, address and date of birth. However, neither the Directive, nor the UK Money Laundering Regulations (MLRs) defines exactly what identity is. It could be possible to adopt an SDD strategy where, providing no other money laundering / terrorist financing risk indicators are present, a non-traditional approach to identity checking is adopted.

Given the legislative permission to use a range of documents and data, and considering the friction introduced into the on boarding process when a new user is asked to share identity documents, firms can, and should, embrace a risk-based approach and look beyond commonly accepted preconceptions about how to verify identity.



Can my business use Social KYC?

The answer is yes, when using the risk-based approach that regulators expect to see.

It can be used on its own, in many cases, for a wide range of e-commerce operators that are not currently obliged (regulated) entities under European AML law. For example, some e-commerce operators are required to have confidence that their services are not being offered to persons under 18. Social KYC can provide such comfort.

For entities regulated under AML where stricter standards are mandated, social KYC can be used as part of a wider compliance and risk strategy that increases the amount of data and/or documents that you collect and verify commensurate with the risks of money laundering and terrorist financing.

Use case for Social KYC for Cryptocurrency

For the purposes of this paper we have constructed a basic hypothetical tiered KYC & IDV construct for a cryptocurrency exchange that is based on the current requirements for e-money and payment service companies - whilst cryptocurrency is not yet fully in scope of European AML rules it is essential that operators in this sector are not perceived to operate a lighter touch approach than regulated electronic money issuers.

An example of a possible risk based and defensible use of Social KYC within the cryptocurrency sector3:

Cryptocurrency Exchange 'ABC' wishes to enable easier on-boarding of its lower value clients, especially from emerging markets, and so creates a tiered KYC structure:

all customers names and addresses are collected and identity is verified against social data4 in addition to conducting sanctions checking and possibly adverse media checks (IDV & KYC Level 0)

customers that wish to transfer to or from their account or hold > EUR1000 in the wallet (local currency equivalent) must also have their addresses independently verified - can be via any platforms that also permit DOB and address verification, such as available social platforms5, Blockchain ID, payment service providers or third party data providers (IDV and KYC Level 1)

customers from higher risk countries outside of the EEA and all other customers are subject to enhanced due diligence requirements including Politically Exposed Persons (PEP) checking (IDV and KYC Level 2)

any persons that are a match for PEP checking and any other customers deemed to be higher risk are subject to a requirement to obtain information or verification of source of wealth/funds (IDV and KYC Level 2)

Fintech firms should consider replacing costly identity verification at onboarding with a social KYC approach that increases the data and/or documents requested and verified based on a risk assessment of territories, products and customers. Users get a more fluid sign-up experience and you get the information you need to adequately identify them based on the perceived level of risk. As long as you have processes and procedures that are justifiable, well documented and consistently applied, regulators will look favourably at your approach. However, you should use this as an opportunity to work with your regulator so that they can understand how new technologies can be used to better manage AML risks.

---

[3] Please note this is not a compliant AML compliance construct 'per se' because AML compliance constructs require detailed consideration of inter alia: country (of establishment, customer and source of funds), customer type and ongoing behaviour, product type, and any additional risk factors. However, we offer it as an example of how you might start to construct a policy to meet KYC obligations relying on new technologies and social data.

[4] The degree of confidence required from the social data verification should also increase commensurate with risk. This means that triangulation or deeper data from one source may be required as customers move up through the risk tiers.

[5] LinkedIn, Facebook, Google+, Amazon, PayPal

Adopting Social KYC: Factors to consider

Social KYC can be an excellent tool for non-regulated entities that are not subject to the requirements of the Directive or Money Laundering regulations (MLRs), but wish to carry out some form of verification of their clients.

Regulated entities who are subject to the Directive and MLRs could also benefit from using Social KYC as part of a risk based approach to their money laundering and terrorist financing obligations under the Directive and MLRs.

A risk based approach

Anyone using Social KYC should ensure that it is appropriate for their business and customers, and should implement it as part of a risk based approach to its KYC and AML / Counter Terrorist Financing (CTF) strategy.

The Guidance, while technically not applicable to non-regulated firms, can be useful in creating an appropriate KYC strategy and should also be considered by firms working in areas that may, in the future, become subject to such regulation, e.g. cryptocurrency firms.

JMLSG recognises that the electronic 'footprint' of individuals can provide useful corroboration of a customer's identity:

> *5.3.35 External electronic databases are accessible directly by firms, or through independent third party organisations. The size of the electronic 'footprint' (see paragraph 5.3.25) in relation to the depth, breadth and quality of data, and the degree of corroboration of the data supplied by the customer, may provide a useful basis for an assessment of the degree of confidence in their identity.*
>
> *(JMLSG Guidance 5.3.35)*

However, the Guidance also states:

> *"For an electronic check to provide satisfactory evidence of identity on its own, it must use data from multiple sources, and across time, or incorporate qualitative checks that assess the strength of the information supplied. An electronic check that accesses data from a single source (e.g., a single check against the Electoral Roll) is not normally enough on its own to verify identity."*
>
> *(JMLSG Guidance 5.3.39)*

This confirms that the use of a single social source for IDV checking is not, on its own, sufficient to verify identity for regulated entity purposes (though it may still be acceptable at certain simplified due diligence levels for some products and in some cases). However, for regulated entities, the use of social IDV from multiple sources in order to gain greater confidence could meet this requirement at both standard and enhanced levels of CDD depending on the data available and the circumstances - i.e. Social KYC can meet the IDV requirements for regulated entities.

Social KYC has its place in a wider KYC strategy allowing firms to analyse multiple sources (LinkedIn, Facebook, Twitter and many more), each of which can offer a deep history that is exceedingly hard to fake convincingly. Each data point (name, location, date of birth etc.) can be corroborated across the various sources in order to assess the credibility of that data.

It is key to note that under the MLRs, an SDD approach is not acceptable in any cases where money laundering or terrorist financing is suspected (or known). If a regulated entity identifies such activity they must make a report to the relevant authority.

Social KYC and the regulators

As more and more people use social media and create an increasingly broad and deep electronic footprint this information will become increasingly valuable as a source of identity and proof of life. As the use of Social KYC becomes more common, strategies can be honed and improved and give users ever greater confidence in its ability to effectively identify their customers. It is essential that operators work with the relevant authorities to ensure they understand how Social KYC can be used to enable financial inclusion, better customer experiences and better electronic data on customers and transactions whilst also managing the serious risk of money laundering and terrorist financing.

> *We've always insisted on our licensee's knowing who their customers are. Software that reliably helps them to do that easily, at the same time as reducing bureaucratic burdens on customers and supporting a focus on key risks, would be most welcome. The important thing for us is that the process is understood by the company using it and is fit for purpose given the profile of the client base.*
>
> *Samantha Barrass, Chief Executive Officer, Gibraltar Financial Services Commission*

Conclusion

Social KYC provides both regulated and non-regulated firms with an additional tool to address and mitigate fraud, manage money laundering and terrorist financing risk, and manage reputational risk. For forward-thinking firms social checks are a cost-effective and robust way to enhance the risk-based approach, and can have a significant positive impact on the customer onboarding process, especially within market segments that traditional identity solutions do not adequately cover or where they are deficient.

With approximately three-quarters of the global internet population actively using social media[7] it is possible to implement robust, risk-based KYC without needing to lose users in the process. Use of Social KYC reduces friction and enables greater confidence and trust with online transactions. It is also a key part of and stage in the trend to federated KYC. Veridu and Ramparts European Law Firm would be delighted to work with you to bring about the change we wish to see in the world.

1 Fore Street,
London EC2Y 5EJ,
hello@veridu.com,
www.veridu.com,
@veriduHQ

2nd Floor,
3 Hardman Square,
Spinningfields,
Manchester, M3 3EB
Tel: +44 (0)161 9149785

[7] Source: *http://www.emarketer.com/article.aspx?R=1009976*