

# The future of regtech

With KYC/AML requirements ever more onerous, operators need to turn to technology-led regulatory solutions while an increasing ecosystem of suppliers is developing around new digital identification solutions

Words | Scott Longley



## "Start here"

Regtech may sound like just another of those awkward amalgams, like fintech, adtech and martech before it, designed to entice unwary investors and give a silicon gloss to a host of otherwise disparate start-ups. Yet under the regtech umbrella there are companies working on technology-driven solutions which hold out the promise of digitising many of the more onerous compliance tasks facing the online gambling sector.

It's an evolving landscape. For all the chatter in the world of digital identification of big data, AI and machine learning, biometrics and even blockchain, the regtech universe is still in its formative stages. The challenge of answering ever more onerous KYC and AML demands throws up new questions and dilemmas even as the increased levels of digitisation continues apace.

The push and pull of regulatory demands in this area is acting as a spur to innovation. With the oncoming rush of the EU's General Data Protection Regulation (GDPR) and its related ePrivacy legislation set to be enacted in May next year, the digi-

tal ID sector in Europe has all the impetus it needs to develop the technologies that might make regulation 'merely' a coding challenge.

Enterprises involved in the digital identification area, biometrics, social media tracking and the ecosystem forming around blockchain and distributed ledger technologies are exploring what the implementation of big data techniques will mean when it comes to data protection compliance. For gambling operators, the rise of regtech offers the prospect of better meeting their current and future compliance requirements, while for the consumer the new technologies offer the prospect of seamless yet secure digital transactions.

### Big data and a tsunami of regulations

Until recently, the processes that governed how operators and their suppliers fulfilled their KYC/AML obligations were largely manual and hugely labour-intensive. "KYC/AML best practices primarily rely on risk-based approaches, meaning a given set of processes are designed to mitigate and protect against a specific risk profile," says Zac Cohen, general manager at Vancouver-based digital identity specialist Trulioo.

He points out that technology advances with regard to big data have transformed the way companies go about handling the information they now have to hand. "It has enabled the gathering and sorting of large amounts of data which can be used in a variety of ways such as predictive analytics, smart decision making, customer verification, risk calculations and fraud prevention to name but a few."

The unsurprising corollary of this big data transformation is that it has been accompanied by what Cohen terms a "tsunami of regulation" which shows no sign of slowing down and which has highlight-



ed the need for tech solutions which can help “catalyse the overall digital transformation”.

“By helping businesses adhere to compliance regulations more effectively and efficiently, regtech is helping fuel innovations that improve, automate, and scale the process within industries that are driven by digital transactions,” he says.

The scale of the digital transformation is such that it is having what Cohen terms as an “unimaginable impact on the market and consumers”. In response, regulators across many industries have found themselves behind the curve and needing to adapt quickly in order to better understand the issues and shape the policies around digital identity and privacy.

“Typically they work hand in hand in continuous cycles,” adds Cohen. “Regulatory change spurs technological innovation – new ways to solve impending challenges, and of course vice-versa where tech breaks create a brand new paradigm and regulatory bodies must react to ensure consistency.”

As the gambling sector is well aware, consistency and compliance are a concept where it might be said the spirit is willing but the flesh is weak. Peter Murray, head of gaming at GBG, points out that in the gaming world operators are spending an increasing amount of time dealing with the “idiosyncrasies and challenges” of multiple jurisdictions.

“If (the regulators) are not comfortable or knowledgeable around technology, then how will they be able to legislate for it in order that we see the benefit for everyone?” he ponders. “How tech and

data combine is key to the advancements around identity and it is important that regulators are aware of what is out there.”

The gambling sector isn’t alone in playing catch-up, says Warren Russell, chief executive of UK-based identity screening start-up W2 Global Data. Like the financial services sector before it, gambling companies are in the familiar position when it comes to compliance-based technology of being burdened by the dead weight of legacy systems. “Gambling operators now find themselves in the same boat as financial services, needing to find reliable, low-cost and innovative ways of complying,” he says.

#### Driving efficiency by better data handling

The benefits of using new technology to better identify, handle and filter the customers coming through the door are manifold. Efficiency gains are compounded by the further standardisation of data and analysis, and as data sets are collected across different territories they become better populated. Finally, by adding machine learning technology to the mix these processes can be forever improved upon.

“We are seeing a massive increase in interest in artificial intelligence [AI] and machine learning,” says Russell from W2. “We are implementing AI to work smarter and remove some of the existing pain points associated with traditional AML checks and make it easier for our clients to manage high-risk users and identify false positive matches.”

Onfido is an identity-verification company founded in 2012 which offers products that are wholly built on machine

**"How tech and data combine is key to the advancements around identity and it is important that regulators are aware of what is out there"**

*Peter Murray, GBG*

## Default setting

**Privacy by default – sometimes called privacy by design – describes what regulators view as the ideal approach that should be undertaken by commercial entities when it comes to how they collect, handle and store customer data. The premise is that firms should bake in privacy such that it is the default mode of operation when it comes to digital identity issues.**

“Once you are using a technology, you have to be mindful that you are handling huge amounts of data and you have to think about how that data is being protected all the time,” says Patrick Rennie, associate at law firm Wiggin.

He adds that operators should be aware that they will need to conduct due diligence on their suppliers in this area. “You need to show you have opted for the best solution, not the cheapest,” he adds.

“Of course, under GDPR the product supplier will also be liable as well as the operator. But the data controller at the operator will ultimately be responsible. I would be wary of believing that third-party data solutions can be the panacea. It can help, but you need to make sure that this is the right technology.”

Elle Todd, partner at CMS, believes that gambling companies are somewhat behind the curve on the issue. “They have to be more open,” she suggests, pointing out that the distinctions between consent and personalisation are one area where there is a deal of confusion. “A lot of this is about data transparency,” she says. “This isn’t anything new. You need to tell people that you are collecting data and what you are going to do with it.”



Patrick Rennie, Wiggan



## SELFIE SECURITY

### Biometrics

A Mitek survey last year forecast that \$3bn of mobile commerce transactions this year would incorporate selfies for authorisation and authentication

learning technology. Head of KYC at the firm Jamie Miles says that the key strength of taking a machine learning approach to the identification area is that with every document processed, the technology becomes “more intelligent and robust” as opposed to the previous static systems which only become more outdated over time.

“Once a pattern is recognised and learnt by the machine, it will scan every single subsequent document for this pattern,” he says. “This means that one fraudulent document discovered may lead to many other unrelated documents being detected as fraudulent if they follow the same fraudulent pattern. The software can therefore verify documents in a matter of seconds with the highest degree of accuracy, wherever in the world they are from.”

A multi-jurisdictional solution has obvious benefits for the gambling sector. Cohen from Trulioo notes that his company’s processes, which are also machine

learning enabled, can verify and validate personal identifiable information attributes against a diverse set of regulatory and jurisdictional compliance backdrops.

“We currently offer age, identity, address, document verification and watchlist screening services through a single API integration (while leveraging) machine learning to help provide insights for custom rule settings for each market and investigating additional ways to optimise the technology and user experience,” he says.

### Tom meet Jerry

Yet for all the digitisation that is now built into identification processes, it remains the case that – to date at least – the technology can only take even this new breed of regtech suppliers so far. “Even with the speed at which technology is evolving, and how critical it is to business, manual process is still a standard part of some operators and some jurisdictional processes,” says Murray from GBG.



Miles from Onfido points out that when it comes to tackling fraudsters it can be a game of cat and mouse where human intervention is a necessary part of the process. "It's a deliberate decision for us to use a hybrid approach in our fraud detection process," he says. "The majority of documents can be automatically processed by our machine learning technology but we also have an expert manual team that can review the small number of cases the machine doesn't recognise."

Effectively, innovation in terms of digital identification doesn't happen in a vacuum and it can be matched by advances being made with regard to digital fraud – and it will be human intervention which is needed to first identify and then counter illicit activity. "The machine by itself won't necessarily recognise a new type of counterfeiting, for instance, but that's when our expert team can step in to re-educate the machine, which benefits all of our clients," says Miles. "Human interven-

tion is desirable in these cases, as it means we can maintain very high completion rates rather than having to reject any documents the machine doesn't recognise."

According to Cohen from Trulioo, having a human contingency has distinct advantages for any organisation. "Activities like frequent training sessions, information sharing sessions, and clear procedures are just a few critical programmes to help turn every employee into an active protector of the businesses sensitive information," he says.

Still, the future of digital identification techniques is very much bound up with advances in technology and at present there are three broad strands of innovation which are set to make their mark on the space. These are biometrics, social media tracking and blockchain.

#### Facing the future

Trulioo recently announced a partnership with mobile capture specialist Mitek



#### TRUSTLESS VERIFICATION

##### Distributed ledger technology

A user can better protect the ownership of their own identity with decentralised data blocks being in their control rather than with companies or other organisations



FCA head office in London

Credit: FCA



# Should gambling regs look at sandboxes?

Back in the spring of 2015, the UK's Financial Conduct Authority (FCA) announced it was forming a regulatory sandbox designed to give companies with new technology and innovations a safe space in which to experiment without the full burden of licensing killing the idea before it got off the ground.

Sarah Harrison, chief executive of the UK Gambling Commission, has previously expressed an interest in the FCA approach but has steered clear of suggesting it might follow the same path. Yet, when it comes to ideas around regtech innovation, it might be that embracing just such a concept and enabling more seamless transactions might come close to fulfilling the Commission's objective of putting the consumer first.

"A sandbox like that established for the financial services industry needs to be led from the top to ensure buy-in from all the relevant parties," says Zac Cohen from Trulioo. "This is an area where we'd like to see the regulator taking the lead to introduce and standardise innovation across the online gaming industry."

He suggests there are numerous benefits. Creating a feedback loop between regulators, providers and operators means some of the industry's biggest issues can be tackled collaboratively.

"Often, innovative solutions are blocked or pushed back because regulators aren't brought in until too late in the process – by making them a part of development from the start, operators can be sure that the new solutions they adopt are fully approved and fit for purpose."

Systems which means it will be able to add a layer of biometric authentication to its current API.

Mitek published a survey last year which forecast that \$3bn of mobile commerce transactions this year would incorporate selfies for authorisation and authentication. It found that only 4% of US millennials currently use selfies to authorise purchases but that 46% said they would like to do so. Also, while only 6% of US millennials said they use selfies to verify their identity, 42% of 29- to 34-year-olds said they strongly prefer taking a picture of their driver's licence instead of filling out a form.

Cohen at Trulioo said the company views biometrics as just another layer to be added to its solution. "Most businesses now are global in nature, meaning it's critical to leverage a technology platform that bridges various methodologies, including for example, traditional and non-traditional data, bio-identity, and now more than ever, mobile," he said.

In June last year, GBG moved to position itself to further exploit the application of biometrics when it bought IDscan, which utilises technology that helps authenticate documents including passports, driving licences, visas and work permits. As GBG said at the time, this is one area where manual processes are being replaced altogether and Murray says it remains an area which is "front and centre" in the company's strategic vision.

"IDscan allows facial recognition as part of the customer journey whether it be at the front end when onboarding or further down the line when accessing your account, with fingerprint recognition on

your iPhone or bank account," he says.

As Russell from W2 points out, though, the technology is still going through a trial phase. "We have on trial a number of facial recognition and biometric products and have ongoing discussions to test the viability and cost of these services," he says. "It is definitely something we will be investing in further in the future, however there are still issues with accuracy and therefore usability in the field together with realistic costs that clients will pay for the technology."

## Tweeting to forget

Each of us leaves a digital footprint via the various social media apps and websites that we frequent and digital identification specialists have already picked up on the commercial possibilities of corralling that information in order to better identify and evaluate individuals.

According to recent estimates from real-time data platform Domo, Facebook has over one billion daily users generating four million posts per minute. Instagram, meanwhile, sees over 1.7 million likes of photos every minute amounting to over 100 million every hour and on Tinder there are nearly 300,000 swipes per minute. Twitter generates 21 million tweets per hour.

As Murray from GBG points out, the slew of data leaves open to question such issues as what exactly the information tells anyone, how reliable it is, how predictive it can be and what value does it bring to those that have collated it. "How we layer that in to an individual's identity enabling individual engagement is one of the more

**"The GDPR is partially a response to the privacy risks created as a by product of the personal data generated by digitisation"**

*Guy Cohen, Privitar*



interesting aspects of the ID space and regulators are starting to look seriously at this," he adds.

Indeed, the regulators are looking at this area in more ways than one. A vital aspect of the debates surrounding digital identity is the attitude of the consumer to the dissemination of personal information. Its latest manifestation comes in the right to be forgotten embedded with the EU's ePrivacy legislation that will come into force with the GDPR in May next year.

A recent survey of UK consumers commissioned by analytics provider SAS found that nearly half of all adults wanted to activate their right to be forgotten under the new rules next year. The poll also showed that the willingness to share anything other than basic demographics fell dramatically with only 19% saying they were willing to share lifestyle and culture information.

### The buzz cut

Which brings us to blockchain. Distributed ledger technology holds out the promise of 'trustless' verification whereby a user can better protect the ownership of their own identity with decentralised data blocks being in their control rather than with companies or other organisations. User-managed blockchain IDs would be given over to those companies or applications strictly according to what aspects of the ID were needed.

"Distributed ledger technologies and blockchain are buzzwords just now," says Russell from W2. "I think that most companies in the fintech sector are exploring these new technologies and how they can be applied. Some of the most creative use of these is likely to come from start-ups which will have the innovation and flexibility to test and explore the capability."

Russell adds that there are many sectors where users want to verify ID characteristics such as age but don't want to disclose other personal information. "In a retail environment, using blockchain to store identity characteristics would allow a consumer to verify that they are over 18 while giving the retailer confidence that the blockchain hasn't been altered or compromised," he says.

One of the new cohort of start-ups working on distributed ledger technology solutions for digital identification is Tradle, which proclaims it is "building KYC on

the blockchain." Chief executive and co-founder Gene Vayngrib says the company's solution is answering some of the tensions that have emerged with GDPR around how companies comply with its provisions regarding data security and consumer choice and other regulatory reporting requirements.

"We can answer something like 80% of these concerns," he claims, suggesting the Tradle solution will offer consumers a view of all their relationships in the market and the mechanism to maintain them.

"On the surface, we kill big data," he says. "Because the data is disaggregated so you can't analyse it in one place. You shouldn't be utilising my pattern of usage across five banks. No-one should be doing that except the individual user."

### Power to the people

In large part GDPR and other legislation regarding data privacy and data security are consumer protection measures. "The GDPR is partially a response to the privacy risks created as a by-product of the personal data generated by the digitisation of most industries over the last 20 years," says Guy Cohen, the policy lead at privacy start-up Privitar.

"I think we are at an inflection point where customers start to see the potential harms which arise from the explosion of recording and processing of their personal data. In the future we expect to see privacy increasing as a competitive differentiator as customers seek out organisations which adopt privacy protecting business models.

He adds that the "winning formula" will be not whether to innovate with personal data or not but instead whether or not to innovate with personal data in a "privacy-preserving way". "The winning business models will be those which can both innovate with data and protect privacy."

The cost of failure in this regard is all too obvious and the gambling sector will hope that regtech's technological success won't come at the cost of consumer trust. As Cohen from Trulioo points out, technology providers have a "higher moral obligation to safeguard personal data and ensure there is never a negative trade-off between adoption and security." The heavy-lifting can be done by the tech – but the finessing will still need a human touch. ■

## What changes does the GDPR bring?

4%

percentage fines as percentage of total global turnover for privacy breach

72

number of hours before a breach must be reported

190

countries affected by the scope of the regulation

28,000

number of new data protection officers required across Europe

Source: Deloitte Risk Advisory – GDPR Vision and Approach