Securys®

Enterprise Insights

KYC, AML and data privacy – a delicate balancing act

One of the great problems in financial services is the misuse of data.

As countries around the world pass new data protection laws and enhance enforcement, compliance teams are facing some challenging issues.

One key issue is whether anti-money laundering (AML) and know your customer (KYC) processes provide sufficient justification for processing personal data.

It's a fruit of the poisoned tree situation. Institutions acquire information, usually for reasons of customer onboarding, or AML, and then it somehow leaks its way out into the sales team. We've now discovered that this asset-rich customer isn't very leveraged and we can now sell to them. Most of the time the banks get caught so the temptation continues. And this is, fundamentally, a problem of natural justice. The idea that people are innocent until proven guilty is what gives criminals room to operate and so there's a constant battle to decide how far into the lives of the virtuous we're prepared to intrude in to catch the sinful.

Pleasing everyone all of the time

There are some big questions to be asked around how it's possible to keep financial services regulators, data protection regulators and – most importantly – customers happy, how to satisfy US regulators and process data lawfully in the EU or UK and what can be done to improve privacy protection without compromising compliance.

AML = Anti-Money Laundering

KYC = Know Your Customer

Institutions acquire information which somehow leaks its way into the sales team.

One of the key problems is that there are two bodies of legislation. There's a body of legislation to do with money laundering and countering the funding of terrorism and preventing fraud. As is common with soft legislation, this organisation is only concerned with those things while simultaneously being overreaching. This creates an environment where banks, sometimes unjustifiably and sometimes justifiably, feel that anything is justified in the pursuit of that end. Which means that they collect a great deal of data and do an enormous amount of processing. They also do a lot of routine surveillance and monitoring and buy data in from third parties.

These banks have had their knuckles rapped by the financial service regulators for not doing enough AML checking. But the consequence of this is that they then do too much.

Going above and beyond

The regulations on minimisation and limitation of purpose say that you should only collect the information that is absolutely necessary for the purpose, that you should be strictly limiting what you do with that information to the purposes to which it was collected. But banks often go above and beyond what the law asks for. Then the law is rewritten or the regulator reinterprets the rules to make necessary what wasn't previously necessary, because everybody's doing it.

A good case in point is the retention of passport copies. What the law originally said was that the financial institutions' authorised officer needed to see identification documentation, verify it and record the fact that they have done so.

Then it became clear that it was quite difficult for banks to demonstrate to regulators that they've done this sufficiently. So they started keeping copies of the passport as a way of evidence in compliance.

Now it's regulatory guidance to keep copies – which is a potential disaster from a privacy point of view because if a bank is hacked, the hacker has everything they need to go and steal your identity somewhere else. The fundamental point is there's this tension between trying to achieve the potentially virtuous end of limiting money laundering and terror financing and trying to comply with the equally virtuous end of respecting people's personal boundaries.

Automation for the people

In order for mortgage decisions to be made quickly, data is fed into a machine, which combines lots and lots and lots of data points drawn from all over the place to decide whether or not you get a loan. If you are being offered an instant decision on credit, it's not being made by a person. Consumers increasingly want a decision within the hour and have their money in their account immediately. There is an extraordinary demand for instant

Since 2007 there have been over 200 cyber incidents targeting financial institutions – a situation which is set to get worse as state-sponsored cyberattacks targeting financial institutions are becoming more frequent, sophisticated, and destructive.*

There is tension between trying to achieve the potentially virtuous end of limiting money laundering and terror financing and trying to comply with the equally virtuous end of respecting people's personal boundaries.

*https://carnegieendowment.org

service and an equal pressure to make sure you don't lend money to people who can't afford to pay it back. Automation is an inevitability. However, routes of appeal don't exist because we don't know yet how the computers have come to those decisions as they've effectively taught themselves. There are also issues around intrinsic bias and machines learning based on the data they've been fed, which, if biased in the first place, will perpetuate. How do we stop machines making biased decisions around potential criminals while also catching the criminals at the speed we need them to?

Good governance and effective controls

The solutions have to do with robust appeal mechanisms, effective controls and good governance. This entails looking into false positives and not just treating a false negative rate as a key performance indicator. In a false positive you have made a mess of someone's life and the consequences of that can be very significant.

It also comes down to technological controls that ensure you protect the information more effectively when you're its custodian. This means proper encryption and redaction.

Watch our webinar

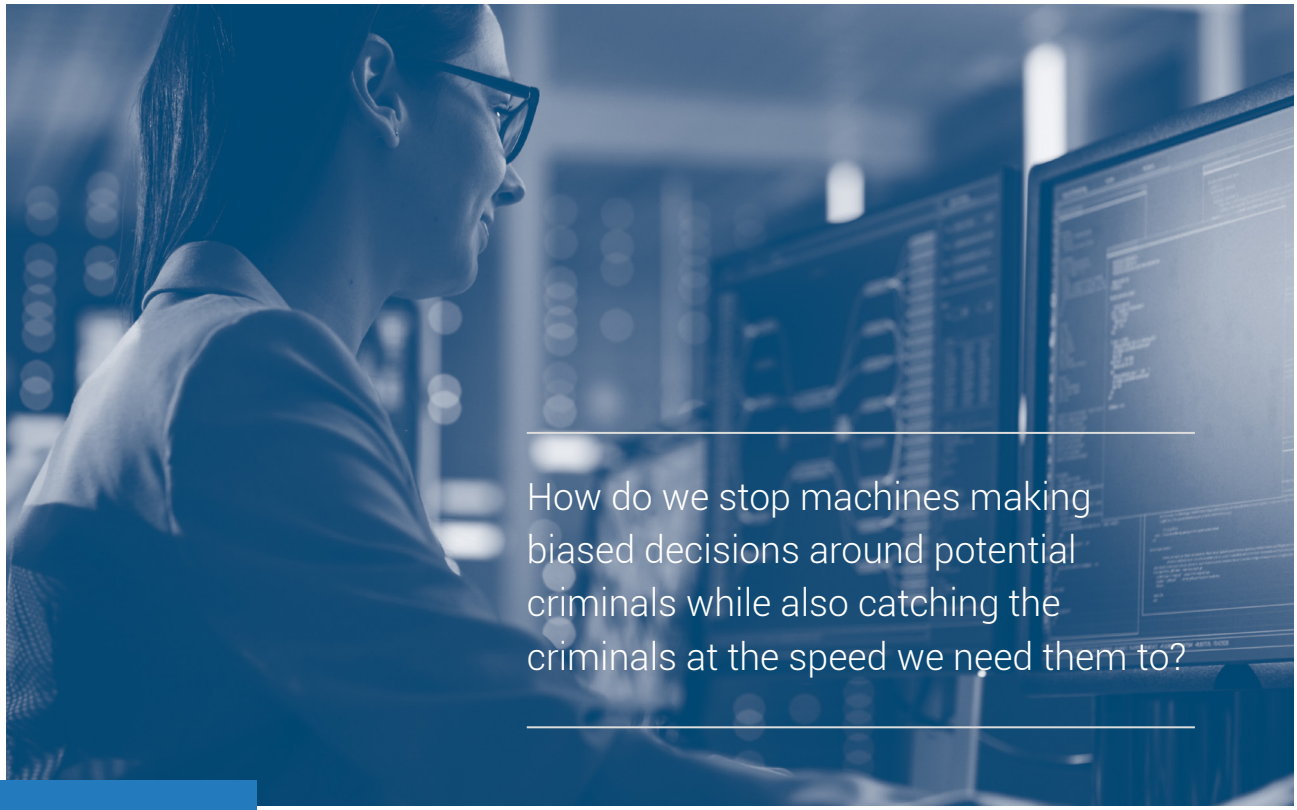
To watch our webinar on KYC, AML and data privacy, visit:

www.securys.co.uk/webinar-kyc-aml-and-data-privacy

And yet banks still aren't doing this. Consumers act on privacy. Good privacy practice can deliver bottom-line benefits and can be used as a competitive advantage. Ultimately, banks should seek to reassure their customers that they're keeping their data safe, while doing their best to counter fraud.

Teeth on both sides

A bigger discussion is needed and this means regulators sitting down and writing a combined AML and privacy rule that works and has teeth on both sides.



About Securys

Securys is a specialist data privacy consultancy with a difference. We're not a law firm, but we employ lawyers. We're not a cybersecurity business but our staff qualifications include CISSP and CISA. We're not selling a one-size-fits-all tech product, but we've built proprietary tools and techniques that work with the class-leading GRC products to simplify and streamline the hardest tasks in assuring privacy.

We're corporate members of the IAPP, and all our consultants are required to obtain one or more IAPP certifications. We're ISO 27001-certified and have a comprehensive set of policies and frameworks to help our clients achieve and maintain certification. Above all, our relentless focus is on practical operational delivery of effective data privacy for all your stakeholders.

Securys®
Privacy Made Practical®

161-165 Farringdon Road
London
EC1R 3AL

T 0800 193 8700
E info@securys.co.uk
W www.securys.co.uk

securys-limited
@SecurysUK

UK0014/0222