Acuris Risk Intelligence

# White Paper

## Expanding Regulatory Reach – How Smaller Financial Firms Handle Compliance Challenges

# Expanding Regulatory Reach – How Smaller Financial Firms Handle Compliance Challenges

As compliance demands expand, Acuris Risk Intelligence is also looking at companies such as asset management firms, challenger and foreign banks and fintech companies, who now also have to consider their compliance obligations. Unlike larger financial institutions, these players do not possess the administrative wherewithal to undertake the internal regulatory checks that their bigger counterparts routinely run, so they have to improvise. Let's take a look at the difficulties these organisations face and how they can adapt their compliance processes.

## ASSET MANAGEMENT

Smaller and mid-sized investment firms have to find shortcuts to effective compliance, as unlike larger financial entities, which have been under regulatory control for decades, smaller companies lack the experience and expertise to adequately meet AML requirements. So, for smaller companies, outsourcing compliance is probably the best option – companies that provide compliance services already have teams that specialise in that area.

Small asset managers should also consider software analytics, which regulators recommend are run routinely as a way of unearthing issues. This also improves data quality and control, since it adds an extra layer of security to a company's compliance framework. There are a wide variety of compliance areas that can benefit from analytics: process management, customer data, financial activity, third party risk, and so on. Integration options also allow companies to operate faster and re-use the same information for more than one task. Looking ahead, predictive metrics, machine learning and AI will also be used to analyse and predict risk and offer appropriate measures. This approach would encompass compliance management, reporting, analysis and monitoring, as well as planning compliance policies.

Technology would also benefit asset managers in client onboarding, streamlining processes and improving the client experience by communicating information in an easier and more convenient fashion. This is key for smaller businesses that rely on reputation and good client relationships.

## CHALLENGER BANKS AND FINTECH

Challenger banks and fintech firms offer a more frictionless, customer-friendly digital experience, but this comes at a price of lower regulatory scrutiny – and this is starting to attract attention. A recent example is Revolut, the fast-growing UK fintech company that offers banking services including a pre-paid debit card, currency and cryptocurrency exchange and peer-to-peer payments. The company raised serious concerns over its lack of compliance, after failing to block thousands of potentially suspicious transactions on its platform[1]. This failure led to an AML crackdown and customers being locked out of currency services, which resulted in a series of complaints and potentially serious reputational damage. This emphasises one major advantage that traditional banking has over challenger banks - reputation. Big banks have built solid reputations over the years and even when faced with major fraud or money-laundering scandals, they have enough reputational credit to recover (examples

[1] 01 March 2019, Antony Peyton, Fintech Futures, *Revolut rocked by compliance and culture criticisms,* https://www.fintechfutures.com/2019/03/revolut-rocked-by-compliance-and-culture-criticisms/

include Bank of China, JP Morgan, Bank of America and many others).

So although online fintech firms offer easier, faster and cheaper options for customers, they have compliance issues. Because they are primarily online, customer verification methods must be improved, including know your customer (KYC) and other AML and due diligence practices. Such checks cannot be postponed to achieve faster onboarding, especially as smaller firms are increasingly targeted by regulators. Fintech companies need to find innovative ways to maintain their ease-of-use *and* to implement the necessary measures to counter financial crime.

The introduction of the Revised Payment Services Directive (PSD2) will help. This EU directive aims to provide a level playing field by harmonising consumer protection and the rights and obligations for payment providers and users. Challenger banks, being more agile and flexible, are at an advantage to big banks here. According to a PwC study[2], two-thirds of banks in Europe are planning to use the new regulation to catalyse change in their core banking operations.

## LACK OF CYBERSECURITY THREATENING ALL FINANCIAL TIERS

Cybersecurity is also a fast-growing threat to all financial services firms, big and small. Data breaches are becoming increasingly common - according to consultants RPC, the number of data breaches reported by UK financial services firms to the Financial Conduct Authority (FCA) jumped from 25 in 2017 to 145 in 2018 – a rise, year-on-year, of 480%.[3]

There are already many laws and regulations in place to counter such risk (The EU General Data Protection Regulation /GDPR/, The New York Department of Financial Services Cybersecurity Regulation, etc.) but these are useless if even governments do not meet their requirements. Earlier in 2019, all Germany's political parties, except for the far-right AfD, were hacked[4].

## CONCLUSION – RISK MANAGEMENT MUST "SMARTEN UP"

Regardless of size, all financial institutions are being questioned by both the authorities and the general public about their compliance protocols. Good compliance programmes take time to develop and must be continually updated as the regulatory framework is adjusted.

So our conclusion is that risk management must "smarten up" and find better ways to detect anomalies and potential threats, faster ways to onboard and identify customers, and more efficient systems to prevent money-laundering and terrorist financing. Automation and AI will be inevitable parts of that process, as will research and the implementation of new technology, combined with information sharing, which, as we have seen, is already a political priority. Last, but not least, reputation will remain a strong factor in company success.

---

[2] PwC, *Waiting until the Eleventh Hour*, https://www.pwc.com/gx/en/financial-services/assets/pdf/waiting-until-the-eleventh-hour.pdf

[3] 26 February 2019, RPC, *Data breaches reported by financial services firms rise 480% in a year to 145*, https://www.rpc.co.uk/press-and-media/data-breaches-reported-by-financial-services-firms-rise-480-percent-in-a-year-to-145/

[4] 05 January, BBC, *German cyber officials defend handling of mass data attack*, https://www.bbc.com/news/world-europe-46768990