Introduction
Automation is now a reality for financial services organisations.

Advancement in machine learning means that many human processes can be replaced, and as this technology improves so will the ability to handle more complex tasks.

Automation certainly has benefits and the promise of cost saving and expediency is naturally alluring to firms seeking competitive advantage. However, we should proceed with caution; whilst the increase of machine decision-making in financial services is inevitable it may not be a panacea.

This paper focusses specifically on automation in financial crime compliance. We discuss the current context of automation in financial crime, its merits, the processes where it may be well applied, the practicalities and the pitfalls. Our objective is to appeal to financial crime professionals in a way that helps cut through the hype and start thinking in a pragmatic way.

Automation in financial crime compliance today
Robotic Process Automation (RPA) is growing fast in Asia where new technologies have traditionally been more readily adopted. The uptake of RPA in the US and Europe has been slower where attitudes to automation are different, particularly due to concerns about people becoming redundant to computers.

As a result of automation we have already seen fewer bank branches on the high street and much less human interaction between banks and their customers. Many services are now fulfilled faster and with more reliability by a machine. And in the main, this has the benefit of improved customer experience and cost efficiency for firms.

Most areas of financial crime compliance have processes that could benefit from automation. Onboarding, monitoring and offboarding all comprise tasks that must be carried out routinely, in high volume and have definitive outputs.

Ensuring robust onboarding and monitoring processes is a priority for many organisations, who risk sizable fines for failing to carry out appropriate Customer Due Diligence (CDD).
Onboarding requires collecting certain information about the client to build a risk-based profile. Required data includes their profession, sources of income, transaction behaviours, whether they are a Politically Exposed Person (PEP) or subject to any sanctions. Where individuals, or entities, pose certain risk then Enhanced Due Diligence (EDD) may then become appropriate.

Once onboarded monitoring of clients is the next important stage. Transactions must be analysed to check for behaviour that might indicate suspicious activity, any new jurisdictions entered must be logged and basic profile information must be checked for any general Customer Due Diligence (CDD) changes.

In most cases, the collection of customer identification and verification data is a very straightforward process that benefits from automation. It is only in certain circumstances, such as where more complex relationships exist, that a machine-based algorithm may fail to detect things that warrant further attention.

EDD also continues to benefit from increased automation. Many organisations typically outsource EDD to an external provider who manually compiles reports. This market is being now disrupted by companies using technology to provide a similar quality of information at a fraction of the cost.

Automation has the potential to bring considerable advantages. The quality and consistency of data can be improved, Ultimate Beneficial Owners (UBO’s) may be identified more quickly, onboarding times are shortened, silos are removed, regulatory changes responded to more quickly and services linked to clients via digital apps. However, automation may only be viable under certain conditions.

Suitable processes for automation must be high volume, to provide economies of scale, be discrete and repeatable, and be deterministic. Where these conditions are not met, human processing may remain the better option.

Despite the value of computer intelligence, it is important to acknowledge that in many cases human decision-making is still superior to even the most advanced machines. Humans can identify patterns in apparently irregular events, they can make quick connections between one system and another, they can consider possibilities and make moral judgements.
The solution maybe a hybrid approach, harnessing the best of computer-based automation and human oversight. Good customer outcomes must remain – for the time being at least – a very human consideration. It is unlikely that the FCA would interview a computer to question why it arrived at the outcome it did.

Such hybrid approaches are starting to be seen, for example in investigations. Workflow is broken down into discrete tasks such as data discovery, analysis, case management and decision point. The more binary tasks are then automated freeing investigators to focus on more complex tasks. The net result is an increase in speed and better first-time decisions informed by improved data collection and analysis.

**The 6 pitfalls of automation**

1. Automation for the sake of it
2. Automate to replace
3. Automate too quickly
4. Automate too much
5. Automate without understanding the workflow
6. Automate without understanding the algorithms

**Six common pitfalls when making automation decisions**

With the potential value automation can bring, organisations are considering how they can implement an effective strategy. However, there are some common pitfalls that could derail an otherwise well intended automation plan.

**1. Automation for the sake of automation**

As with all new technologies there is a wave of hype to begin with. Providers aim to capitalise on the latest industry trends with new products and services and work hard to persuade buyers of their merits. Firms seeking ‘first-mover’ advantage jump onboard with the latest tools and techniques and it is easy to get swept along losing sight of objectives and requirements.

There is no imperative for firms to automate, and taking time in making a considered decision mitigates risk. Decisions to automate should be based on a thorough assessment of needs and a full review of how these needs could be met, through automation or otherwise. Efficiency gains can often be made without the need for innovative technology, but by simply reviewing current processes and seeking opportunities to strip out unnecessary activities.

Wholesale automation is certainly not the answer. Firms should rationalise what and why they have automated, and be able to articulate this to the regulator.

**Firms should rationalise what and why they have automated, and be able to explain this to the regulator.**
2. Automate to replace
Automation will often reduce headcount and on this basis, may be championed by the finance department as a cost saving initiative. However, when automating anything within financial crime compliance, there must be a better rationale than that, with the quality of outputs remaining the primary consideration.

Only where all the conditions are suitable, should automation be considered. For example, determining the impact of sanctions and PEPs is a complex process with many interdependencies. This is something which benefits from a human approach; one that is methodical, reasoned and can handle ambiguity. This process would not be a suitable candidate for automation. Firms seeking only to reduce budgets may unintentionally compromise their compliance.

3. Automate too quickly
When a decision to automate is made there is often a desire to realise benefits quickly. This is an easy trap to fall into. However, automation can have both positive and negative transformative affects. Care needs to be taken to ensure that the right candidate processes are selected, that automation happens in a controlled way and that the interfaces with automation are adequately prepared. This includes the compatibility of legacy systems and processes, and importantly how automation will be integrated into the culture of the organisation.

Robust project management should be observed along with a test-and-learn approach. Whilst this may add time to the roll out process, it puts the organisation in control, mitigating risk and ensures in the longer term that the most effective solutions are delivered.

4. Automate too much
Automation is not suitable for everything. Within financial crime compliance, automation is still developing and we are a long way from establishing best practice. There are many solutions offered by many vendors but none represents a proven total solution. Firms need to thoroughly consider their context, including their means, objectives and current ways of operating. Adopting a healthy amount of scepticism is a good starting point. Automation should be considered as a possible option rather than de-facto. It needs to earn its place as a viable alternative to other options and once implemented it must be tested and measured to ensure that it is delivering the expected benefits.
5. **Automate without understanding the full workflow**

Many organisational processes have evolved over time. They may be inherently inefficient with unnecessary steps or may even have failed keep up with requirements.

Automation on its own does not fix bad processes. Before considering whether to automate a process should be fully understood. Mapping workflows helps to reveal gaps, dependencies and inefficiencies; and ensures that should a process be automated it can be effectively implemented and reviewed later.

Automation is likely to involve cooperation with IT partners, either internal or external to the organisation. While they will be capable in automation technology they are unlikely to know financial crime compliance processes. It is important to work closely to develop detailed and complete specifications and ensure that the automated solution performs as required under rigorous testing.

6. **Automate without understanding the algorithms**

Automating a process involves breaking it down into a series of rules based steps or algorithms, which based on inputs will return certain outputs. It is important to understand how these algorithms behave and what are their limitations.

At any time, the regulator can ask for justification of how a decision has been reached. It is equally important to be able to explain this and provide a robust rationale when a process has been automated.

Also, it should be appreciated that inaccurate data inputs will give rise to poor quality outputs, and algorithms will provide spurious results when put to work on analyses beyond their design. When relying on system generated outputs it is wise to understand how they have been derived so retaining some level of criticality.

**Conclusion**

The growth of automation of simple manual processes in financial crime compliance is inevitable, it enhances efficiency, speed and consistency. These affects are positive for firms and their customers.

However, there are pitfalls. The advantages of automation will only be realised by firms who develop a considered plan and implement it with care. Organisations need to set realistic expectations and determine exactly how automation can be best applied to their own set of circumstances. It is critical to keep in mind that whether a process is automated or not, a firm is still responsible for ensuring high quality and compliant outputs.
The market for automation is rapidly evolving and we are far from establishing best practice. The financial crime industry is still grappling with what and how to automate and there are many solutions available. The challenge for financial crime teams is to understand what technology can bring and how then to integrate it into their organisation. Once implemented it can be difficult extract technology and wrong decisions can have long term negative impacts. By carrying out a detailed needs assessment and being thorough in reviewing the capability of suppliers, the right solutions can be selected to build fit for purpose future proof frameworks.

There are cultural concerns with automation, which may be perceived as a threat to job security and resigning control to machines. Rational or not, these concerns are present and should be met with sensitivity. Automation can be used to empower staff, by reducing the time spent on simple routine tasks and freeing time to focus on more complex activities. As a result, job roles can be re-designed to become more meaningful for employees. This may involve training to understand how to incorporate automation and its outputs, into wider processes.

Whether you’ve already introduced automation or you’re considering how to, we hope that this paper has provoked thought. We’re always interested in other perspectives so please do get in touch to share your views and experiences of automation in financial crime compliance.

Jan Hagen
MANAGING DIRECTOR, RFS FINANCIAL CRIME
Jan has over 20 years’ experience. He has worked at leading consultancy firms advising senior executives how to mitigate financial crime risk. He specialises in helping clients to implement the right technology solutions as well as leading on training, investigations and remediation programmes. Jan is a Fellow of the International Compliance Association.