

What a RegTech Compliance Killer System Will Look Like

By **Bernard Lunn**

CEO, Daily FinTech

Compliance is a big, ugly problem, and it is getting worse, and nobody has nailed it yet. In short, compliance is a tremendous opportunity. Investors say: 'Show me compliance deals'. Bankers say: 'Show me a solution'. Financial technology (FinTech) companies say: 'We must spend our precious cash on lawyers and regulatory experts'.

Nobody loves compliance. Everybody hates compliance. That is why it is a massive opportunity. Like a cure for cancer or cheap and abundant renewable energy, the problem is easy to state, but the solution is far, far harder to build.

We have seen a lot of regulatory technology (RegTech) solutions, but we have yet to see the killer system. We see lots of lawyers and outsourcing firms willing to throw worker-hours at the problem. We also see lots of point solutions. These are, at best, putting bandages on the wound.

So far we haven't found a killer solution; however, we do know what a killer solution needs to look like. There are five attributes that we detail later, after presenting a requirements checklist.

Before detailing the checklist, here are the seven reasons why compliance is so hard.

1. *It is a moving target.* Since the financial crisis, we have had lots of new regulations and lots of new scandals (which trigger new regulation). At the same time, we have the emergence of bitcoin, which is entirely uncharted territory.
2. *It is a territorial hairball of complexity.* Finance is a global business, and 'bits do not stop at borders'. However, money does

stop at borders, and each country has its own spin on regulation. There are even cross-border variants such as Islamic finance. Each is critical. Put them all together, and the result is seriously nasty and complex, and in a global economy, that is the reality we have to deal with.

3. *It is an easy lever for politicians to pull.* Beating up bankers is a natural vote catcher. The negatives from too much regulation are not so visible, and causation is unclear. So it will always be a moving target, and it will still get more complicated.
4. *It is a cross-cutting concern.* Like cyber security, compliance cuts across every system, including ones written before most of today's regulation was even a gleam in the eye.
5. *It does not have a revenue line attached.* Despite the massive risk posed by compliance failure, there is no revenue line from which a banker can grab budget.
6. *It is an existential threat.* Get it wrong, and you could be gone tomorrow. So, nobody loves spending money on compliance, but you have to spend money on it.
7. *It is functionally complex.* There are so many areas to understand, and each is complex on its own – money laundering (know your customer [KYC]), tax (Foreign Account Tax Compliance Act [FATCA]), consumer protection, data privacy, and systemic risk (Dodd-Frank Act). Add them all together, and it is a recipe for sleeping like a baby (waking every few hours screaming).

The following is the high-level five-point checklist for a great RegTech compliance solution:

1. *Real-time data in context.* Big data is just so-called digital landfill unless it is delivered just in time and in context. 'Just in time' means that the data is made available in real time even if it is not consumed in real time. It is not relevant until it is relevant in context (which is why it is not always consumed in real time). For example, consider a conflict of interest statement. The fact that a family member just moved into a conflict of interest position is

useful only if delivered within the context of a system where you need to declare any conflicts.

2. *Legacy integration.* Any solution that involves changing the legacy system is a showstopper. It is the weakest link issue. Just one legacy system that is not integrated could be your compliance nightmare. Combining 1 and 2 (real-time data in context plus legacy integration) is tough. Rewriting all apps to be compliant is expensive and takes too long. Doing integration according to the constraints of decades-old middleware and batch-based core systems is hard but essential.
3. *Understanding the risk/reward trade-off.* Perfect compliance is like perfect security. Designing an ideal compliance system is straightforward. Any bureaucrat can do that. The problem is that you will stop the business as all customer-facing processes grind to a halt, or you instead encourage people to ignore compliance rules and just pay the fines as a cost of doing business. In the real world, there is a trade-off between compliance and frictionless onboarding. When creating a compliance solution, you need marketing growth hackers on the team as well. You have to enable internal people, customers, and partners to all do their jobs without putting the business in great danger.
4. *Immutability.* A shared database where all parties can trust that nobody can change the data it contains is a big deal. This is where blockchain technology could be a breakthrough, although there is no need to use blockchain technology to get a distributed and immutable (append-only) database.
5. *Rules-based user interface for non-programmers.* Apart from death and taxes, we can be confident that compliance rules will change and grow in complexity. Unless a compliance person can 'code' these rules using legal language rather than programming code, any solution will quickly become obsolete.

There are two big reasons for optimism. The first is the perennial one that, with technology getting better, faster, and cheaper every day, some entrepreneur will create a compliance killer system that meets the aforementioned five attributes – the prize is certainly big enough. This is an article of faith, similar to saying that we will get

a cure for cancer or cheap and abundant clean energy without knowing how we will get there.

The other reason for optimism is based more on the observable fact that the regulatory environment is getting easier.

Yes, you read that right. I wrote that the regulatory environment is getting easier.

The reason is that politicians, fearing citizen backlash, are starting to rein in the worst bureaucratic tendencies of regulators. For a long time, entrepreneurs faced competition, and regulators sent them the rule book. Regulators were government employees who thought about competition only in the abstract. Today, the environment is more fluid, as governments recognize the economic return on innovation regarding jobs and gross domestic product (GDP) growth. The regulators now face real competition because their political masters have to keep citizens happy, and citizens care about employment and GDP growth. With both FinTechs and global banks being increasingly mobile, jobs can disappear fast if regulators get it wrong. Plus, innovation is the primary driver of productivity, which drives GDP per capita.

Pity the poor regulator who must balance that with protecting citizens from fraud and abuse. This has led to two positive developments:

First, simpler and unbundled regulation in many countries. Unbundled regulation means you could get a payment license, or a deposit license, or a current account license.

Second, tech-smart regulation. Two examples are the second Payment Services Directive (PSD2) in Europe and payment bank licenses in India. This moves from 'throw the paper rule book at your compliance team of lawyers' to 'send standards docs and application programming interface (API) specs to your tech team'.

FinTechs and small and medium-size enterprises (SMEs) will drive change. Incumbents and corporate entities can throw lawyers and outsourcers at the problem. This is not an option for FinTechs and

SMEs. This is where tech-smart regulation is critical. Consider the eXtensible Business Reporting Language (XBRL).

Real-time Data Machine-readable Streams for Regulators

In the wake of the financial crisis in 2008, the US government mandated machine-readable financial reports via XBRL. That was a wonderfully progressive move that could dramatically change the efficiency and reliability of the capital markets by bringing financial reporting into the twenty-first century. Then came the backlash, with politicians claiming to save small businesses from the burden of regulatory compliance.

To understand why this is baloney, travel with a financial data item through the financial reporting process:

Step 1. Start as an electronic bit in an accounting/enterprise resource planning (ERP) system. The data is now perfectly machine readable and gets aggregated and processed most efficiently.

Step 2. The data is converted into a human-readable form for the Securities and Exchange Commission (SEC). For many companies, the only time their numbers are on actual paper is when they send their reports to the SEC.

Step 3. Somebody extracts the data from a PDF or HTML file and turns it back into a machine-readable bit in XBRL format.

That ‘somebody’ is probably working for an outsourcing firm that is being paid by the company doing the reporting because it has to comply with the SEC mandate.

Step 3 looks more like a burden that should be eliminated. However, the solution is *not* to eliminate Step 3. *The solution is to eliminate Step 2.* Technically this is simple.

Imagine the poor overloaded folks at the SEC surrounded by piles of paper. They are dedicated, smart, and hardworking. They will therefore have evolved a system that sort of works – poring over individual company filings and marking something odd about a data item in a footnote with a yellow pen, and then digging through a pile of documents to look on page 256 of another report (having cleverly marked the page) to correlate something odd on that other company’s filing ...

Imagine if all the data was in XBRL electronic format and they could let an algorithm do the grunt work so that they could do the higher-level work needed to catch the bad guys and maybe avoid a repeat of the financial system’s ‘cardiac arrest moment’ in September 2008.

The algorithms could process thousands of companies to look for that anomaly, that weird thing that says, ‘something looks fishy’. The data surfaced by the algorithms still require the higher-level cognitive and pattern-matching skills of humans. This is about empowering the SEC staffers to be more efficient. I imagine that they would vote for this change.

The work done by SEC staffers is impossible without better systems. The devil is in the details, or to put that in financial reporting language, the devil is in the footnotes (where a company buries that embarrassing fact it wants investors and regulators to gloss over).

Forward-looking regulations will eventually leave behind the cute constructs of the analogue age – paper and batch cycles – and demand data streams that they can parse as needed in real time. In the meantime, compliance has to deal with both the new real-time world and the legacy batch world, and history teaches us that legacy sticks around a lot longer than anybody anticipated.

Sharing the KYC Burden for Small Business Through Digital ID

Compliance is a pain for BigCo, but it is a manageable pain. It is impossible for SMEs, which do not have significant compliance departments. That is why we see change being driven by SME needs. This is starting to happen through partnerships. A natural fit could be a large telecommunications company partnering directly

with a challenger bank. Telcos are hungry to diversify into new revenue streams amidst an increasingly digital landscape, and they are the natural repositories of digital identification (ID) (which is the key to KYC). Once the digital ID problem has been solved, the rest of RegTech is a lot easier. Digital ID remains a thorny issue, with societal-level problems around privacy, but these can be resolved with technology, and it is likely that forward-looking telcos will drive that change because the mobile phone is the key to digital ID.