A Guide to Regulatory Compliance & Reputation Management for **Emergent FinTech Companies**

rdc | KEMP LITTLE

Introduction

Disruption is the motivation behind all things FinTech. Scores of start-ups are re-inventing financial services, attacking legacy 20th Century (if not older) banking paradigms and building better, faster and cheaper 21st Century platforms. Technology is defining the new competitive advantage for finance. Say farewell to banking, investing and lending as we know it.

Often lost in this whirl of innovation is regulatory compliance. It certainly isn't as exciting as architecting the next payment platform. And, it may even get in the way of creating the next great thing. But it cannot be ignored. You cannot innovate around it. The reality is:

- Regulations governing financial transactions, particularly economic sanctions and anti-money laundering/counter terrorism, apply almost as much to FinTech companies as they do to traditional banks.
- The cost of non-compliance for FinTech startups is potentially catastrophic. Yes, fines can be quite large and egregious conduct may be met with criminal penalties; but the real harm is worse: regulatory hiccups will crush valuations, limit your ability to complete your next capital raise, and potentially cause you to fail.
- There is an enormous opportunity here. Bringing the same entrepreneurial spirit to regulatory compliance will only enhance your burgeoning competitive advantage. Banks for years have struggled with regulatory compliance for the exact same reason they are ripe for disruption of their core model: their legacy technology platforms are too burdensome, wedded to the old way of doing things and never fully incorporated regulatory compliance into their core. Instead, they try to "bolt on" compliance measures, adding costs and delays to processing times. Just imagine if you could incorporate state-of-the-art compliance processes into your new paradigms. Better, faster, cheaper compliance side-by-side with better, faster, cheaper finance. That would be a real disruptive force.

In this e-Book, Regulatory Data Corp (RDC) and Kemp Little explore all three of these tenets so the FinTech community can understand their regulatory obligations, align their compliance efforts for success and exploit best practices to its advantage.

Contents

An Overview of the Current Regulatory and Enforcement Landscape

Why are technology companies regulated?

Money laundering is not just a bank problem but an issue for any company, however small, that engages in activities that involve the transfer of money. In money laundering, criminals take "dirty" money from illegal activities and "launder" it by placing small amounts of money into the legitimate financial system and then moving the funds around to obscure their origins. Smaller less traditional firms may be particularly vulnerable to being used for money laundering, as their structure may make it easy for small amounts of money to be transferred quickly. This would be the case, for instance, with peer to peer lending, where money may be lent and paid back fairly quickly. Money launderers may see technology companies as 'easier' targets than big banks.

Overview of regulation

If your business involves the transfer of money for clients, then you may well be required to comply with AML and counter terrorism laws. These are a set of laws at European Union and national levels that elaborate on one basic guideline: do not let your firm be used to launder money or finance terrorism. At the EU level, the Third Anti-Money Laundering Directive (AMLD3) applies; at the UK national level, the following laws implement the AMLD3 obligations:

1. Money Laundering Regulations 2007;
2. Proceeds of Crime Act 2002; and
3. Terrorism Act 2000.

In the spring of 2015, the Fourth Anti-Money Laundering Directive will come into force to change some of the existing rules. The end goal remains the same: certain types of firms operating in the financial sector must take steps to ensure that they are not used by money launderers and/or terrorists to channel funds from or toward criminal activity.

The threshold question is whether your firm needs to be concerned about complying with AMLD3 (used here as shorthand to refer generally to the set of laws governing AML). AMLD3 applies to a wide variety of companies, including credit institutions (basically, banks) and financial institutions. "Financial institutions" is a broad category that includes firms offering services that involve the transfer of money, such as lending, money transmission services and the issuing and administering a means of payment, like credit or other payment cards. In other words, if you are in the business of moving money back and forth among clients and yourself, you should be aware that AMLD3 may very well apply and seek professional advice.

If your firm is required to comply with AMLD3, then you should focus on the following four basic requirements:

1. Identify your customers (no anonymous accounts!) with an appropriate level of "due diligence";
2. Keep records of due diligence and transactions;
3. Train staff to guard against money laundering and terrorism financing (have written procedures in place so that everyone knows what to do and whom to contact); and
4. Report suspicions of money laundering or terrorism financing to your assigned regulator (without tipping off the suspects).

Identifying Customers

You will need to identify customers in the following two situations:

1. A "business relationship" is established (in other words, the firm and the customer will be doing business with each other on an ongoing basis); or
2. The customer and firm have entered into a one-off significant transaction or series of transactions that are connected, which amount to more than a set value.

Identifying your customer is more involved than simply taking down a name and address. You must identify:

1. all those individuals
2. with whom you have a business relationship
3. or who own 25 per cent or more of the entity with whom you do business.

If you do need to identify the customer, then you need to ask yourself, just who is the customer? And how risky is doing business with him? Sometimes identifying the customer is straightforward, as when the customer is a human being who is physically present and produces standard documents like a passport and utility bills that confirm his identity. At other times, however, the process requires some detective skills.

A key area of concern arises when the customer is an entity (a corporation, trust, organisation, etc., as opposed to a natural person). This is because the AMLD3 requires firms to identify the "ultimate beneficiary." By ultimate beneficiary, the AMLD3 means the natural person who is at the end of whatever chain of entities owns the party doing business with a company. In other words, if your customer is another business, say Acme Ltd., you will need to ascertain the identities of all the human beings who own or control that business. If it turns out that Bcme Ltd owns Acme Ltd., you'll need to go up the chain of owners until, eventually, you find a real live person.

Not all individual owners need to be identified or investigated: only those individuals who own or control 25 per cent of a company are subject to this rule. Not surprisingly, this process is time-consuming. AMLD4 will lighten the burden by requiring EU member states to keep central registers of those beneficial owners, which will simplify the process.

Due Diligence

Once you have identified the customer, you'll need to conduct "due diligence". This means assessing just how risky it is to do business with this person, or, put in other words, how likely is it that this person will be using your company to launder money or shift funds to terrorists? Due diligence involves an assessment of a variety of factors, such as the type of business and customer. Just how intensive your investigation needs to be depends on the level of risk posed. Customers will generally fit into one of the following three categories:

1. Simplified due diligence;
2. Standard due diligence; or
3. Enhanced due diligence.

AMLD3 considers that certain types of individuals pose less risk than others and makes an exemption to the due diligence requirements so that only simplified due diligence needs to be carried out for customers fitting in those categories. If, for example, a customer is itself subject to AMLD3, or is a company whose securities are listed on a regulated market, the usual rules do not apply. This will, however, change under the AMLD4, which will require simplified due diligence to be justified on the basis of a risk analysis.

On the other hand, enhanced due diligence is always required in the case of "politically exposed persons" (PEPs). These are defined as persons who hold public office and are considered to be more at risk for corruption than others because of their position. Not only is the actual PEP considered to pose a higher risk, but his family (parents, spouse, children and their spouses) and close associates are too. At this time, domestic PEPs are excluded from automatically being considered high risk. AMLD4 will expand the PEP category to include both domestic and international PEPs.

Sanctions – An Additional Concern

In addition to identifying customers to comply with AMLD3, you should also be aware of the "sanctions" lists. Sanctions screening is separate from your obligations under the AMLD3 but no less important. The sanctions lists are lists of those individuals and/or organisations who are known to be involved with criminal or other undesirable activity. These lists are made public by the government and updated regularly. Your obligation is to avoid doing business at all with any person or entity who appears on these lists. This requirement often goes beyond your customer to include anyone your customer transacts with. This is why most firms rely on screening solutions that check all parties in a transaction that flows through your systems.




Monitoring and Reporting

Once you have duly identified your customer and entered into business with him, you are obliged to monitor the transactions and the relationship on an ongoing basis. A system must be in place to ensure that any suspicious activity is reported to the appropriate authorities. If you suspect that a transaction is related to money laundering or to terrorist financing, you may not carry out the transaction. You will need to report the transaction to the appropriate authorities without delay and without saying or doing anything that might alert the customer that you are reporting them. If halting the transaction would tip off the customer, then you may complete the transaction as long as you alert the authorities immediately afterward. The ban on disclosure covers third parties as well as customers.

Risk-based approach

In implementing AMLD3, companies are instructed to take a risk-based approach rather than a checklist approach. This will be even more the case under AMLD4. In other words, compliance with AMLD3 requires more than simply ticking off boxes; rather, a risk-based approach requires you to evaluate all of the different factors that may contribute to the level of risk posed by a customer or transaction. The focus is on the goal of combating money laundering and terrorism-financing, not on blind compliance with rigid rules. The touchstone is the question, what are the risks inherent to our business relationship with this particular customer?

To answer this, you should look to a variety of factors and then weigh them up against each other to get a complete picture of the risk involved. As a guideline, you should ask questions that cover the following areas:

1. The customer;
2. The customer's location; and
3. The nature of the products and services.

In other words, you should focus on the risks posed by the customer (your neighbour or someone you've never met?), his location (United Kingdom or Afghanistan?) and the nature of the products or services. More specifically, you should be considering questions such as:

1. What is the type of customer? (Is this an individual who is known personally, or a faceless entity on the internet?)
2. The type of beneficial owner? (If the customer and beneficial owner are connected through a complicated chain of entities, is this justified by business reasons?)
3. The nature of the business? (Is this a high cash-flow business?)
4. Issues associated with the geographical location of the customer or business? (Is the customer local or based in a high-risk jurisdiction?)
5. The delivery channel? (Online? In person?)

Some other factors that a company can look to in assessing the customer include:

1. Source of wealth
2. Source of funds
3. Reputation of individuals and companies
4. Nature of and level of account activity
5. Political connections

These are not the only questions that you should be asking; however, these are examples of the types of questions that will allow you to assess the risk posed by this customer. Having a complete picture of the risk posed by customers and their transactions allows you to allocate your resources more effectively, by investing more heavily in high-risk areas than in low-risk areas.

The Consequences of Non-Compliance:

What happens if companies do not have AML systems in place? Failure to comply with AMLD3 can result in serious penalties, fines or even criminal prosecution. Authorities will impose fines – sometimes to the tune of hundreds of millions – upon companies for failing to have adequate AML systems in place. Even individuals, such as those who are responsible within a company for monitoring and reporting suspicious activity, may be fined individually if they fall short. In the last few years, the Financial Conduct Authority (FCA) has issued fines of hundreds or even millions of pounds to banks.

Note that the penalties are not for allowing money laundering to occur. Fines have been issued for not having an effective AML system in place. The focus is on ensuring that companies have an effective AML system in place rather than the specific outcomes.

The internal investigation and remediation costs associated with an AML breach can be massive, and senior management and commercial time is diverted from running the business. Reputational risk is, for many firms, now perceived as a risk on par with regulatory risk.

Where to Start: Key Components Required in a Robust Compliance Programme

An effective compliance programme is not a one size fits all exercise; you will need to tailor your compliance programme to your firm's needs. In general, however, you'll need to invest in the following:

1. Due diligence on customers
2. Ongoing monitoring of customers and transactions
3. Governance arrangements that clearly allocate responsibility for money laundering issues;
4. Strong guidance from senior management on the importance of the firm's AML processes;
5. Training of staff
6. Money Laundering Reporting Officer

Besides due diligence on customers when embarking on a business relationship, you need to continue monitoring the customer and the transactions with them on an ongoing basis. In high risk situations, monitoring should be more frequent and more intense than in low-risk situations. The results of the monitoring should be recorded and any issues raised with the appropriate person. Where a firm uses an automated monitoring system, you'll have to be aware that you may not be able to rely entirely on the system but will need to ensure that the results are subject to review by humans.

What happens if a transaction is flagged? If monitoring uncovers a suspicious transactions, you'll need to report this to the appropriate national authorities. All staff will need to understand the procedure for escalating suspicions. This means that you'll need to provide guidance and training on how to recognise suspicious transactions, how and to whom to report these, and the obligation to do so without disclosing suspicions to the customer or third parties.

The impetus for the monitoring and reporting must come from senior management, who must give strong guidance and make it clear that AML is a priority. This can be effected by regular training for staff, depending on their roles. You must also appoint a money laundering reporting officer, who needs to be given both sufficient resources and the independence to do his job.

Implementing an Anti-Money Laundering & Know Your Customer Programme

Once you have completed your regulatory and risk management assessment you will then move to the delivery phase of your project. The success of a project can be helped significantly by recognising that there are a series of challenges you need to be aware of and the importance of selecting the right delivery partner to make sure your AML and KYC programme is a success.

Typical Challenges

Emergent FinTech companies face an interesting challenge – AML/KYC compliance is an inherent element of the product proposition due to the online, and therefore anonymous, nature of the business, yet the processes and controls that make up a robust programme are often at odds with the entrepreneurial spirit of this sector. The challenge is, therefore, how to implement a programme that strikes the right balance between keeping the company safe and facilitating innovation and business growth – all while managing cost, time and workload.

Cost

The idea that compliance is expensive to achieve is a misconception driven by media reports of the ever spiraling budget and resources banks are dedicating to their AML programmes. The need for banks to continually increase spend on compliance is the result of the outdated, on-premise legacy technology platforms that are so deeply embedded within their organisations. Designed over a decade ago, these costly solutions are still being used to manage today's, very different, regulatory obligations. Rather than reviewing the validity of their compliance technology, banks are throwing more money and people at the job to cope with the tremendous workload, and to keep regulators satisfied.

Celent estimates that 75% of the global IT spend of banks in 2015 will go towards maintaining legacy systems, this includes spend related to keeping up with new regulations.

(http://thetally.efinancialnews.com/2015/02/fn-fintech-focus-much-banks-spend-new-tech-investments/)

Over the past decade technology has evolved at a startling pace giving FinTech companies the opportunity to build their compliance programmes on rentable, Compliance as a Service platforms. These platforms offer cost-effective implementation, maintenance, configuration and scalability and, when combined with the right data and services, unrivalled protection from risk.

Time

Time is of the essence for new and growing businesses. Reducing time to delivery is critical in driving customer satisfaction and growth. Attracting new customers is almost entirely dependent on a business delivering a faster, more efficient service than traditional providers. For businesses touting quick and easy access to their services as a competitive advantage, money transfers for example, it is especially important to implement a KYC programme that carefully balances optimum levels of protection with efficiency in customer onboarding.

For many new businesses, the simplest and quickest route to ensuring compliance may appear to be subscribing to an online service and manually checking new clients, members, and other third parties against regulatory data, including sanctions and Politically Exposed Persons. However, the remarkable growth being experienced by many emergent FinTech companies means manual processes quickly become inefficient and unsustainable due to a lack of staff and resources. When this happens, there is a real danger that the pressure to achieve growth targets can lead to corners being cut to support business growth.

Regulation requires that you have in place fit-for-purpose and proportional compliance programmes. If your policies, procedures and controls are found to be deficient, regardless of whether a breach has occurred, you are likely to be fined or penalised. The ensuing financial and reputational damage could be impossible to recover from.

Workload

Perhaps the most challenging aspect of AML/KYC compliance is managing workload. As your customer or member base grows your onboarding programme will return more hits, some of which will be false positives, but all of which must be investigated thoroughly and promptly in order to meet the stringent expectations of regulators.

There is good news however and, as previously mentioned, all regulatory guidance is focused on companies implementing a risk-based approach to compliance – starting with a risk assessment. The results of your assessment will inform you of where your most serious risks are coming from – perhaps specific countries, services or customer types present a higher level of risk to your business and warrant more attention. This insight allows you to tailor the level of customer screening you perform so that it is proportionate to the perceived level of risk. So, low risk customers receive your basic level of screening, while high risk customers are investigated more thoroughly. This approach significantly reduces workload and ensures your limited resources are focused where they are needed.

Selecting the Right Vendor

For the reasons outlined above, selecting the right vendor is crucial to the success of both your compliance programme, and the company. As a compliance officer, you must have the utmost confidence that your client screening is identifying the risks you need to know about. This is dependent on screening clients against the right data, using the right parameters to focus your efforts on the most critical risks, and being able to investigate any alerts promptly to keep the onboarding process fluid.

Keep things simple and opt for a vendor who covers the four key pillars of a compliance solution:

- ☑ A scalable compliance technology platform with a ready-built workflow that you can get up and running quickly.
- ☑ The ability to instantly screen and monitor all customers against risk data that is specifically relevant to your business and your view of risk.
- ☑ A sophisticated filtering engine that supports a risk-based approach and allows you to configure screening to the results of your risk assessment.
- ☑ Access to specialist services when you need support clearing and investigating alerts.

The Four Pillars

Technology Platform

FinTech companies should seek out vendors with the same qualities as themselves – innovative, nimble and responsive to the evolving needs of clients. Your technology platform should encompass all of the following attributes:

- **SaaS** – Increasingly adopted by national and global financial institutions, cloud-based solutions offer many benefits including lower cost of ownership and minimal implementation times compared to deployed systems which, along with the timescales and complexity, are often more expensive to maintain than they are to install.
- **Security** – Make sure you have full insight into how your vendor protects your client data from loss or mis-use at all times.
- **Scalable** – Look for a solution that can scale up as your company grows, and that can easily accommodate your growing client base or new risks without a significant increase in cost.
- **Configurable** – Your company is growing and changing day by day and your technology platform must be easily adaptable to meet your evolving needs, without the need to hire in expensive consultants.
- **Workflow** – Save time and drive productivity by opting for a platform that comes with a pre-built compliance workflow.

Risk Data

Access to a broad set of risk data gives you the ability to drive the value of compliance by extending the scope of client screening to identify reputational, business and financial risk as well.

Understanding the criteria used by a vendor to build their database is crucial as the vast majority of data providers have deliberately limited their coverage to regulatory risks. This has been done to help clients manage their workload, as in many cases bigger databases generate more results, most of which are false positives. However, since the inception of these databases over a decade ago, filtering technology and analytical modules have advanced considerably and can be precisely configured to meet the specific needs of individual organisations. This enables companies to choose a broad risk database and rely on technology and superior analytics to eliminate irrelevant results far more effectively than before.

Key elements to consider when selecting your risk data are:

- **Full protection from regulatory risk** – Ensure the database comprehensively covers global sanctions, watch lists, and Politically Exposed Persons (PEPs) – the risks that regulation requires you to screen for.
- **Risk-scored PEPs** – PEPs make up the largest set of regulatory data and therefore generate the highest workload. However, the definition of what makes someone a PEP is very broad and ranges from heads of state all the way through to local public office holders. Look for a database that includes risk scoring of PEPs based on a variety of criteria such as seniority, country risk level and any negative media associated to a person. Risk scores can be used to filter out lower risk PEPs to reduce workload.

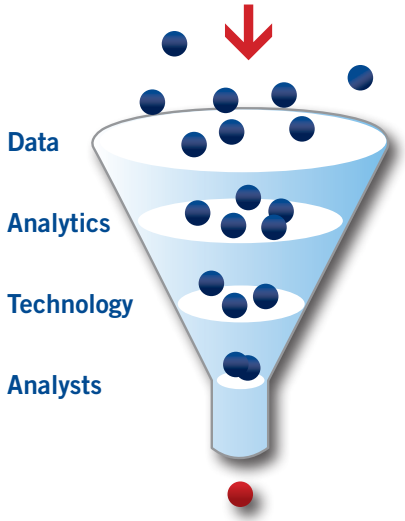
- **Brand Protection** – Your risk assessment will have provided you with good insight into the reputational, financial and business risks facing your organisation. Make sure these are comprehensively covered by the database you opt for and can be incorporated into client screening seamlessly and efficiently.
- **Highly structured data** – As previously mentioned filtering technology can now be precisely configured to eliminate irrelevant results. The more granular the categorisations you use, the more precisely your screening rules can be configured in line with your risk based approach. Look for a vendor that clearly categorises the risk or crime type as well as the stage of risk (arrest, trial, conviction etc.). This allows you to check for the most critical risks facing your business - for instance, terrorism or money laundering - at the earliest stages when persons are alleged or accused to have been involved in such crimes, and touch less critical risks only when they grow to a more material stage.

Filtering Engine

Client screening is primarily based on matching the names of your prospects, members and clients to names on a global risk database. However, simply relying on matching names can result in a high level of false positives and unnecessary work for you. A good filtering engine will allow you to screen on multiple criteria – date of birth, gender, country to name a few – which helps to refine your results. A best-in-class screening engine takes this much further allowing you to set up precise rules based on risk type, stage, severity and location. This level of sophistication ensures you can automatically filter out irrelevant results without running the risk of missing a true hit.

Key considerations when evaluating filtering engines are:

- How easy it is to set up your filtering rules and tweak these as your company evolves?
- Can you incorporate risk stage (accusation, arrest, trial, conviction etc.) into your screening rules?
- Can you set different screening rules for different levels of risk? For example, your risk assessment may have informed you that certain services that you offer expose you to higher levels of risk, and potential customers should therefore be screened more thoroughly, using broader parameters, than customers of a service that presents a very low level of risk.
- Can you automatically monitor all customers and members on a daily basis for changes in their risk profile? A monitoring service that runs in the background, only alerting you to changes that you want to know about will give you the peace of mind that your risks are covered while you focus on your core business.



Servicing Platform

You need to maintain the highest levels of productivity to steer your organisation to success and your internal headcount should be focused on innovation in your core business, not routine administrative work. That is why it is critical that your vendor provides a helpful hand. You need a full compliance platform – data – technology – analytics – and services to complete your mission.

Services are key to this, and in the 21st Century, there is no reason for you to do the "grunt work" – like reviewing false positives, checking "white" and "black" lists and prioritising processing. Have your vendor do it.

Critical to your success is the skill of the vendor's staff in performing these tasks. You must have absolute confidence in the experience, skills and abilities of the individuals carrying out work on your behalf and you must ensure that:

- Analysts are formally and thoroughly trained, and ideally have previous experience and the relevant qualifications.
- All work is done strictly in line with the rules and processes you have developed as part of your compliance programme.
- Results are delivered to you in a comprehensive alert with supporting material to speed up your decision making.

Drive Business Value from Compliance

Trust and reputation are crucial to the success of emergent FinTech companies. Mistakes made in your risk management process can have a serious impact on your ability to succeed

We have already touched on the need to opt for a risk database that goes beyond purely regulatory requirements. Many companies and individuals involved in crime will not appear on sanctions or official lists, but have the potential to cause irreparable reputational or financial harm to your organisation. Access to a deep and broad database of companies and individuals who have appeared in global media in connection with criminal activity will be your best defence.

In March 2014, the US Department of the Treasury's Office of Foreign Assets (OFAC) sanctioned Gennady Timchenko as one of sixteen Russian government officials involved in the Ukraine conflict. However, a scan of global media reveals Mr. Timchenko had been arrested for failure to pay more than 25 million euros in taxes four years earlier.

Incorporating adverse media is your best defence to not only to spotting entities that could be a significant regulatory risk but also significant commercial risks as well.

Conclusion

With US$8 billion forecast to pour into FinTech firms by 2018; better, faster and cheaper financial services providers are poised to revolutionise banking.

Transitioning your company from startup to ‘grown up’ requires access to the necessary capital and investment, and central to this is maintaining an attractive valuation.

FinTech companies that are tempted to sideline compliance to focus on innovation and growth are at severe risk of, not only regulatory penalties, but massive reputational damage that will turn investors away and potentially result in the downfall of a business.

Seeking expert advice on meeting your regulatory obligations; fully assessing your exposure to money laundering and customer risk; and selecting a vendor who will alleviate the burden of compliance are your keys to success, and the time to start is now.

[1]http://www.accenture.com/Microsites/fsinsights/capital-markets-uk/Documents/Accenture-Global-Boom-in-Fintech-Investment.pdf

RDC
emea@rdc.com
+44 (0)20 7959 2243

Kemp Little
info@kemplittle.com
+44 (0)20 7600 8080