fourthline

WHITE PAPER • AMSTERDAM, OCTOBER 2020

KYC Remediation: Mistakes and Best Practices

Regulatory scrutiny obliges banks to re-validate existing clients. Done right, it leads to better customer data and less fraud —but done wrong, it can be the ultimate money pit.

Highlights and quick facts

- Regulators across multiple jurisdictions have turned their attention to the Know Your Customer (KYC) and Customer Due Diligence (CDD) files of existing bank clients.

- Once in the crosshairs of a regulator, a bank needs to act quickly and decisively—often in the face of an imminent deadline.

- Common mistakes banks make when initiating a remediation project: putting the burden on clients, recruiting expensive, untrained staff, trying to build a file with patchwork data, and relying on manual processes.

- Best practices for a successful large-scale remediation process include rewarding clients, improving data quality, and prioritizing cost and time.

Regulators' latest preoccupation: remediation

In 2019, 58 anti-money laundering (AML) penalties were handed down globally, totaling $8.14 billion—with these figures expected to increase in 2020[1]. In fact, AML fines have growing steadily since 2015, with no slowdown in sight. An August 2020 study by financial consultancy Duff & Phelps concluded that the fines handed out in the first half of this year were imposed for exactly the same procedural shortcomings that regulators have been flagging since 2015: due diligence on new customers, management of AML measures, monitoring of suspicious activity, and ensuring compliance with the rules[2].

Nick Bayley, head of UK regulatory consulting at the firm, observed: "We see the same areas being sanctioned again and again . . . Despite the repeated messages in these enforcement cases it's clear that market participants are continuing to struggle with their obligations."

Under the EU's 5th Anti-Money Laundering Directive (5AML), banks are required to take a risk-based approach to safeguarding the financial system. This has led to a new requirement for KYC/CDD files, whereby banks are required to maintain an audit trail for the risk scores assigned to every single client.

Traditionally, banks have conducted new account onboarding as a binary flow in which the client either fails or passes. If the client passes, most of the time the risk assessment details are not preserved. Under the 5AML, this is no longer permissible.

In the past two years regulators in some jurisdictions (most notably the Nordics, UK and the Netherlands) have started to increasingly focus on the quality and completeness of existing client records—including documentation of risk assessment.

A well-known Western European bank was forced by regulators to perform KYC remediation on a significant number of retail clients due to the lack of an audit trail substantiating a "low" risk rating. This meant that the bank was suddenly faced with an obligation to collect and validate identity data for millions of clients.

> "One of the greatest challenges with these situations is that they create overnight urgency to act."

One of the greatest challenges with these situations is that they create overnight urgency to act. Once the letter from the regulator falls on the doormat of the bank, the clock

[1] https://www.acfcs.org/fincrime-briefing-aml-fines-in-2019-breach-8-billion-treasury-official-pleads-guilty-to-leaking-2020-crypto-compliance-outlook-and-more/

[2] Financial Times - 10 August 2020

starts ticking. In fact, it is not uncommon for regulators to designate an offboarding date: i.e., any client that has not passed KYC remediation by that date needs to be offboarded, putting the reputation and revenue of a bank at risk.

Common mistakes that banks make

The most common mistakes banks make when launching KYC remediation projects revolve around spending money on "window dressing" instead of on strategic solutions that address the root cause of their regulatory failures—often because this seems like the cheapest and quickest way out of the dilemma. In practice, though, this only prolongs and exacerbates the conditions that led to the situation in the first place.

1. Putting the burden on clients:
Consumers generally perceive old-fashioned KYC processes to be a burden the first time around, when they open an account. When banks require existing clients to go through such a process again, it is often met with resistance, dissatisfaction, and even churn. To make things worse, many financial institutions have not shied away from threatening their clients with offboarding deadlines (leading to public displays of outrage on social media, as several recent posts have shown) as well as resorting to intrusive non-digital tactics. For example, one major credit card issuer experimented with sending couriers door-to-door to attempt to re-verify millions of cardholders—a method it quickly found to be prohibitively expensive and time-consuming (not to mention an unwelcome intrusion for customers).

2. Recruiting expensive, untrained staff:
A common step banks take is to aggressively ramp up the hiring of KYC analysts to handle the workload of a remediation project, either in-house or through a business process outsourcing (BPO) partner. The challenge is that the time pressure and sheer size of such undertakings have a negative effect on both the cost and quality of such hires. It often results in hiring unqualified, inexperienced staff to work through "tick-the-box" exercises[3]. Mikael Bjertrup, the head of financial crime prevention at Nordea Bank Abp, says banks initially ramped up compliance so fast they were not able to focus on efficiency in those departments[4].

On the cost side, we have seen situations in which a headhunter poaches a candidate from a permanent contract, places that candidate at a payroll company, which then places the candidate at a BPO player, which then contracts the candidate to a bank. As a result, the fully

[3] https://www.nrc.nl/nieuws/2018/09/28/de-witwasjagers-van-ing-geen-ervaring-geen-financiele-achtergrond-a1916406

[4] https://www.bloomberg.com/amp/news/articles/2020-07-26/bankers-who-profited-from-nordic-hiring-boom-now-in-firing-line

loaded cost of this worker increases by 10x.

When it comes to quality, there are simply not enough experienced people in almost any local market to supply candidates that can hit the ground running. While this is also true for building compliance teams in general, training becomes an even greater challenge under the time pressure created by regulator-mandated KYC remediation situations. The less automated and more customized the processes are at a bank, the longer the training period will be to get new recruits up to speed.

3. Trying to build a file with patchwork data:

Many traditional banks are encumbered by complex legacy IT systems, through which it is notoriously difficult to gather and look at data holistically. We have seen examples at a prominent global bank where the KYC team is examining one set of data, the fraud team another and the transaction monitoring team a third—with no sharing of data between the three teams.

If the starting point of a remediation project is to locate and unify all of the existing data held on each client across multiple systems, this is a recipe for running over your budget and expected timeframes.

4. Relying on manual processes:

Using patchwork data subsequently leads to a tedious and error-prone process in which the newly hired (and overly expensive) staff go through tick-the-box exercises by sifting through disparate bank systems to pull together a CDD file that meets the minimum requirements for compliance.

While this approach may suffice based on the letter of the regulations, it will fall far short of the spirit of the regulations. In the end, the exercise should be aimed at helping banks identify clients that present a high or unacceptable risk to the integrity of the financial system.

> “...the exercise should be aimed at helping banks identify clients that present a high or unacceptable risk to the integrity of the financial system.”

This requires a fundamentally different approach to retrieving, analyzing and interpreting data, as we will see in the next section.

Best practices for a successful remediation KYC project

While most common KYC remediation mistakes involve choosing expedience over quality and putting too much attention on cosmetic changes instead of value-added strategic investments—our recommendations for success involve maintaining a focus on the stakeholders and metrics that matter the most.

1. Reward clients:

What if a bank could promise that the next KYC process would be the last ever? What if a bank customer could leverage data shared with their bank to access other (financial) services? What if a bank customer could become a partner in protecting their account and the accounts of others? What if all of the above could be offered to a client through a remediation process that culminated with the issuance of a re-usable, portable electronic ID (eID)? This would be something for consumers to get excited about—and if it is achievable in under 90 seconds, conversion rates would skyrocket.

Under the European eIDAS (electronic IDentification, Authentication and trust Services) framework, the legal opportunity to provide clients with a reusable eID already exists. We have already seen significant traction with itsme in Belgium, for example. The technology is already available for eID capabilities to be rolled out by banks in a secure and scalable manner. Offering a bank-branded eID allows banks to reuse KYC files internally (e.g. retail banking and SME banking), enables a bank customer to share select data points by consent with an external organization (e.g. full name and address) and offers unrivalled protection against account takeover fraud, phishing and money mules. Such technology is available on a white-label basis, which allows banks to retain control over branding and client ownership while fast-forwarding a decade in the approach to KYC.

2. Improve data quality:

In the mobile-first era, banks lack face-to-face client interaction, but in return get easy access to data points that can help improve the quality of their (centralized) CRM and reduce financial crime. The value lies in looking at these data points holistically. This allows for consistency checks, statistical anomaly flagging, and suspicious pattern identification (since money launderers never work alone).

> “If you see more, you know more—and if you know more, you see more.”

The advancements in fraud prevention and detection technology have not gone unnoticed to fraudsters. There has been a noticeable improvement in the quality of fake documents, and they will only continue to get more difficult to detect. Even some national police organizations are assigning less and less value to an ID document on a standalone basis and relying more on biometrics and contextual data to establish the true identity of a person.

Banks have a privileged position when it comes to data, as they are one of the few commercial organizations that are obliged by law to identify their clients and—by definition of the product they offer—maintain access to a trove of data points throughout the customer lifetime.

If the right data points are retrieved, stored and monitored after a remediation process, a bank can lift its anti-financial crime efforts to new heights. Challenges like money mules, deep fakes, phishing attacks, eBay fraud and many other (new) forms of financial crime can be tackled most effectively by using data. If you see more, you know more—and if you know more, you see more.

3. Prioritize cost and time

In recent years, banks across Europe (with Northern Europe leading the way) have made significant advancements in digitizing their account opening processes for clients. Remote onboarding has rapidly become the standard following the rapid switchover to mobile-first. On the back of this, a number of regtech and fintech startups have introduced solutions to capture and authenticate the ID documents and selfies of clients in a user-friendly manner. While not all of these technologies offer the level of quality and detail a bank requires, there are a number of emerging providers that focus specifically on financial services—meeting the standards needed to convince regulators that they can fulfill their expectations.

> “The efficiency gains of such scalable technologies can lead to cost savings of over 90%.”

However, in a large-scale remediation process, being able to provide a digital experience to account-holders is not the key challenge. The key challenges are meeting time and quality expectations across an entire backlog of client cases. A bank wants to ensure that it gets it right the first time, exceeding regulatory requirements from a quality perspective while also meeting the deadline to avoid forced account closures.

Delivering on time requires an ultra-efficient process, not just for clear-cut cases but also for edge cases and

investigations (e.g. to validate a potential hit on sanction lists). The focus of banks has recently been on hiring thousands of staff to increase capacity, but the big win in capacity comes from reducing handling times. Tech-forward KYC providers can contractually commit to SLA turnaround times measured not in months, weeks or hours, but in mere minutes.

While a typical remediation process may prioritize time over budget, the fact that millions of clients need to be reviewed means costs can easily spiral out of control. In a typical BPO set-up, the vendor (usually a consultancy or audit firm) has very little incentive to increase efficiency, since they are paid based on the total number of labor hours used.

Selecting a tech-driven solution (either pure SaaS or a tech-based end-to-end-solution) instead allows a bank to benefit from technology innovations for back-end processes—not only to filter out ID fraud, ID theft and colluding criminals, but also to reduce the handling time of more complex cases like the aforementioned investigations. The efficiency gains of such scalable technologies can lead to cost savings of over 90%. In a multi-million client remediation project, this means tens of millions of euros in expense reductions. At a time when costs at a bank are a key focus, such relatively easy cost savings are as rare as they are welcome.

About Fourthline's KYC Remediation capabilities:

- Efficiently remediate your existing customer base with our automated and scalable solution, no matter how complex your KYC remediation project. Fourthline has helped leading European banks and fintechs clear their remediation backlogs and achieve compliance in a timely and cost-effective manner, checking 210+ data points at 99.995% fraud detection accuracy.

- Fourthline's risk-sensitive solution eases the burden on low risk customers, ensures that adequate information is collected for higher risk customers, and triggers manual intervention only when required. By segmenting customers more finely, Fourthline enables clients to set appropriate remediation activities, choosing between proactive and reactive contact with customers and determining necessary monitoring procedures and controls.

- Our automated solution also extracts information from old customer records for validation or pre-population, efficiently cleanses all data, removes contradictory facts, and creates a single, valid customer data record with a full audit trail.

- Fourthline's self-serve customer data and biometrics portal—available through our white-label mobile app, mobile SDK, or web SDK—enables banks to be up and running within one week.

Trusted by banks, online brokerages, insurers and leading fintechs, Fourthline verifies millions of identities for customers like N26, DeGiro, Solarisbank, Flatex, ING, and many more.

To learn how we can help with your remediation project or any other digital identity needs, please contact us at info@fourthline.com.