KYC 2020 SEEFAR

WHITEPAPER

Cost of KYC List Screening for AML Compliance is No Longer Out of Reach

How small and medium size financial entities can cost effectively add KYC List screening into AML regimes

Originally published 2017 · **Updated April 2026** · KYC2020 LLC

APRIL 2026 UPDATE

This edition updates enforcement data through 2025, adds a new section on cryptocurrency & digital asset compliance obligations, reflects the expanded FATF membership, and introduces AI-driven screening developments — while preserving the original case studies and core analysis.

In today's fast-changing AML regulatory environment, small and medium size financial services companies face increasing scrutiny and need cost-effective tools to satisfy regulatory bodies. This paper explores how KYC List screening — the cornerstone of any AML regime — is now accessible and affordable for organizations of any size.

Background

Prior to 9/11, adequate AML compliance — and in many cases outright non-compliance — had been *Business As Usual* for most banks and financial institutions. The Financial Action Task Force (FATF), a body which now includes **40 member nations**, was still in its infancy prior to 9/11. It wasn't until 2012 that the FATF actually codified its recommendations and interpretive notes into one document.

This was about the time we saw a shift with various regulators to increase the compliance framework along with imposing stricter fines. These fines forced a shift for most major financial institutions — who had been lackadaisical with their compliance regimes — to recognize the far greater cost of reputational risk.

The Escalating Cost of Non-Compliance

Global AML, KYC, sanctions, and CDD-related penalties totalled $4.6 billion in 2024 — with North America accounting for 95% of that figure and penalties to banks increasing 522% year-over-year. In H1 2025 alone, fines jumped a further 417% compared to H1 2024, totalling $1.23 billion globally. This is no longer a risk confined to the largest institutions — regulators are casting a wider net across neobanks, MSBs, payment processors, crypto firms, and insurance companies.

The landmark case that defined the reputational stakes for earlier editions of this paper was Western Union's 2012 fine of $186 million, which wiped nearly 40% off its stock price in two days. That record has long since been eclipsed. In October 2024, **TD Bank faced penalties totalling approximately $3 billion** — the largest AML fine in US banking history — for systemic failures in transaction monitoring and customer due diligence. As part of the settlement, TD Bank's US operations faced growth restrictions including a cap on asset expansion. The message is clear: the cost of non-compliance now extends well beyond fines to structural operational consequences.

So what about smaller and mid-size Financial Institutions, Money Service Businesses (MSBs), and other financial services entities required to comply with AML/KYC regulations? Most fall into one of three categories:

- Have exited cross-border transactions and other higher-risk businesses due to regulatory risk
- Continue to operate without a compliance framework, or
- Have implemented rudimentary home-grown or grossly inadequate 3rd-party systems, betting that the probability of a fine remains low as regulators focus on larger players

Cost of Compliance =

(Cost of Internal Compliance Infrastructure) + (Cost of Fines) + (Cost from Loss of Reputation) Where (1) Cost of Internal Compliance Infrastructure refers to the total hard and soft costs for running the compliance apparatus — human resources, systems, controls, audits, and loss or delay in business; (2) Cost of Fines refers to FinCen, FINTRAC, AUSTRAC, and other governing body related fines; and (3) Cost from Loss of Reputation refers to the loss in sales and shareholder equity that a business suffers upon discovery of lax compliance standards — including, as TD Bank's case illustrates, regulatory-imposed growth restrictions.

The common theme for most smaller entities is that the cost of compliance continues to be perceived as greater than the cost of fines. This persists because most major vendors and systems are designed and priced for large banks. Smaller banks, MSBs, and other financial services entities face solutions that are too complex to integrate, too broad in scope, and/or too expensive.

Since 2012, the dynamics have shifted decisively. The probability of any given regulator fining a small to medium size entity has increased as larger entities have largely come into compliance. These smaller entities can no longer survive by using inadequate AML tools for the base KYC List Screening function — and since 2025, enforcement activity has expanded to sectors that previously flew under the radar, including fintech, crypto, gaming, and insurance.

Introduction

The key piece of an effective AML regime is Know Your Customer (KYC) screening. This involves searching known public databases and lists for both onboarding and ongoing monitoring. These databases and lists are published by regulatory bodies, governments, and Law Enforcement — including the FATF, OFAC, SDN, UN, INTERPOL, FBI, US Treasury, HM/FCA, and literally tens of thousands of Terrorist, Criminal, Sanction, Watch, No-Fly, and Politically Exposed Person (PEP) lists.

For small and medium size Financial Services entities, existing KYC List screening incumbents typically charge between $5,000 and $10,000 USD annually — and these services usually come loaded with add-ons and features that will never be used. The result is a tug-of-war between the cost of compliance and the risk of non-compliance as it relates to operating a profitable business.

KYC screening services must also offer the flexibility for multiple delivery modes: (a) on-demand screening via web UI, (b) bulk screening via batch processing, and (c) integrated screening via open and extensible API for 3rd-party and in-house system interfaces. List aggregation and normalization is the primary requirement for minimum KYC Screening compliance, but the intelligence and flexibility of the screening engine greatly improves overall compliance efficiency — without the exorbitant costs typically associated with the existing incumbents.

This paper will explore:

- A sampling of key databases and lists as they relate to regulatory bodies, governments, and Law Enforcement
- How these lists are normalized to be accessible and searchable via the web
- Case studies on the ways to access KYC Screening cost-effectively
- The emerging compliance obligations around digital assets and AI-driven screening
- Conclusion and next steps

New Frontier: Cryptocurrency & Digital Asset Compliance

Since this whitepaper was first published, an entirely new compliance category has emerged that directly impacts small and mid-size financial entities, fintechs, and MSBs: **cryptocurrency and digital asset screening**. This is now the fastest-growing area of regulatory enforcement globally.

Illicit cryptocurrency transactions surpassed $24 billion in 2024, and regulatory scrutiny has intensified sharply in response. The crypto sector accounted for the majority of all AML fines in H1 2025, with penalties exceeding $927 million in just six months. High-profile cases have resulted from a "growth at all costs" mentality — where platforms onboarded millions of users with minimal KYC or sanctions screening, ultimately resulting in nine-figure penalties and criminal liability.

Jurisdiction	Framework	Impact on Small/Mid Entities
European Union	MiCA — Markets in Crypto-Assets Regulation	Crypto service providers must register and report suspicious activity. KYC/AML controls mandatory.
United States	FinCEN / BSA — DeFi platforms proposed as financial institutions	Any entity touching crypto flows must screen wallet addresses and transaction parties.
Global (FATF)	Travel Rule — IVMS101 for virtual asset transfers	Originator and beneficiary data must be screened on all crypto transfers above threshold.

The practical implication for any small or mid-size entity is straightforward: if your customers transact with crypto at any point — or if you are a fintech, payment processor, or exchange — you now require a KYC screening platform capable of screening both named parties *and* wallet addresses against sanctions and PEP lists. This is not optional; regulators across North America, Europe, and Asia Pacific have made clear they will not distinguish between traditional financial institutions and digital asset businesses when it comes to AML enforcement.

AI-Driven Screening: Reducing False Positives

One of the most significant developments since this paper was first published is the application of artificial intelligence and machine learning to KYC screening. Where earlier-generation tools returned large volumes of false positives — requiring expensive manual review — AI-powered screening engines can now apply behavioral analytics, confidence scoring, and contextual decisioning to dramatically reduce analyst workload.

This is particularly relevant for small and mid-size entities, where compliance teams are lean. A screening solution that floods analysts with false hits is nearly as operationally damaging as having no solution at all. Modern platforms — including KYC2020's DecisionIQ — now combine list screening with AI-based decisioning, adverse media monitoring, and case management workflows that make compliance achievable without a large dedicated compliance team.

What to look for in a modern KYC screening platform: AI-driven false positive reduction · Adverse media and negative news screening · Wallet address / crypto screening · Ongoing monitoring (not just onboarding) · API-first integration · Audit-ready case management · Risk-based decisioning and tuning

Databases and Lists

Who are the regulatory bodies, governments, and Law Enforcement that publish this data?

Regulatory Body / Government / Law Enforcement	Databases & Lists
United States US Treasury · FINCen · OFAC · CIA · FBI · SDN Each State Financial Regulator (51) · Office of the Inspector General	Sanctions · Money Launderers · Terrorists · Criminals · No-Fly Wanted · Abuses · Weapons · Narcotics · Non-Proliferation · Exclusions · PEP
European Union + EU AML Authority (AMLA) — established 2024	Restrictions · Sanctions · Terrorists · PEP · MiCA Registrations
United Kingdom HM Treasury · FCA	Terrorists · Sanctions · PEP
Canada FINTRAC · OSFI	Sanctions · Terrorists · PEP
Australia AUSTRAC	Sanctions · Terrorists · PEP
Switzerland State Secretariat for Economic Affairs	PEP · Sanctions
Global FATF (40 member nations) · UN · INTERPOL · Egmont Group	Terrorist Financing · Money Laundering Typologies · Criminal Networks PEP · High-Risk Jurisdiction Lists
Digital Asset Registries (New) Chainalysis · Elliptic · OFAC SDN wallet addresses	Sanctioned wallet addresses · Illicit crypto transaction networks DeFi risk flags · Exchange risk ratings

There is currently no single public regulatory body compiling all known sources of Terrorist, Sanctions, Criminal, Watch, PEP, and Digital Asset risk data into one list. With over 220 countries in the world — 40 actively involved in the FATF and over 180 agreeing to implement AML regulatory regimes — these lists and databases will only grow bigger and more complex.

Normalization of Databases and Lists

Given that there is no single standard format for these databases and lists, the data must be normalized so it can be effectively searched. The reality is that all search fields reduce to four basic types of information:

Name	Individual or corporation, including aliases and transliterated variants
Address	Physical, mailing, and registered address
Identification	Drivers Licence, Passport, IBAN, wallet address, LEI, etc.
Date	Date of Birth, Date of Incorporation, Date of Issuance

KYC2020 also accounts for "Additional Data" or "Comment" fields found in so many of these databases. By first screening the core 4 fields for likely hits, then searching the additional data fields for each of the 4 items, there is no need to narrow searches to a specific document type — if a match exists, it will be found. With over **600+ global data sources**, this comprehensive approach ensures no relevant entry is missed.

Summary of Case Studies

KYC2020 is a customer-focused company. The following three cases illustrate the challenges and solutions for small and medium size businesses seeking cost-effective KYC screening that meets regulatory requirements without enterprise-scale pricing.

CASE 01

Pay-As-You-Go

Challenge

The client's KYC List Screening was the bare minimum. To comply with FINTRAC regulations, it needed a more robust tool beyond OSFI lists and Google searches for new client onboarding.

Solution

KYC2020 introduced the client to its Search and Scoring Engine (SSE) via a free 30-day trial with 25 free checks/day. With 600+ global data sources satisfying FINTRAC requirements, KYC2020 created a PAY-AS-YOU-GO option allowing the client to purchase blocks of searches to be used at any time.

Pricing: **$1.25 – $2.00 per search**

CASE 02

Batch Processing

Challenge

The client had a well-defined AML Workflow, successfully audited by regulators and external auditors. They needed an affordable replacement for their batch screening process at scale.

Solution

KYC2020's SSE was validated against their AML Workflow during a free trial. KYC2020 then created a BATCH option, allowing the client to submit an unlimited number of screening requests per day — dramatically reducing per-search cost at volume.

Pricing: **$0.05 – $0.15 per search**

CASE 03

API Integration

Challenge

The client needed seamless integration into their existing proprietary onboarding and compliance systems, with no manual intervention and unlimited throughput.

Solution

After validating on the free trial, KYC2020 created an API integration option, allowing the client to submit unlimited requests per day through their own system with full programmatic control over the screening workflow.

Pricing: **$0.50 – $0.75 per 10,000 searches**

Benefits Across All Three Delivery Models

- ✓ Fits easily into existing manual and IT system-driven AML workflows
- ✓ Ensures adequate controls are in place to meet regulatory requirements for KYC List Screening
- ✓ Reduces the cost of implementing KYC List Screening regulatory requirements
- ✓ Scales from a handful of daily checks to millions of API calls — same platform, no migration
- ✓ Audit-ready case management with full decision trail for regulatory examination

Conclusion and Next Steps

Small and medium size businesses no longer need to muddle through manual list checks or justify the exorbitant cost of enterprise KYC screening tools. The compliance landscape has never been more demanding — fines are larger, enforcement is broader, and new obligations around digital assets and

AI-driven fraud have raised the bar further. But the tools to meet these demands have also never been more accessible.

KYC2020 has built a platform that meets — and exceeds — the needs of small and medium size entities, while delivering the most comprehensive and cost-effective single source for AML list screening compliance. From pay-as-you-go to full API integration, from basic sanctions screening to AI-driven decisioning and adverse media monitoring, the platform scales with your compliance obligations.

Get Started — Free 30-Day Trial

Sign up for a free 30-day trial at kyc2020.com. Try the service to see if it meets your needs. If it does not, we will work with you to come up with a solution that does. By adding an automated tool for KYC List screening, you will save your organization significant manual effort and reduce the risk of regulatory fines — or worse, business disruption. The cost of doing nothing has never been higher. sales@kyc2020.com · kyc2020.com

Originally published 2017 · Updated April 2026 ·