RegTech Business Models

Selling shovels to the compliance gold-rush — the rush ends, the shovels stay

Digital Finance

vs.

The Prospectors

We have to dig through all of it!

The Shovel Sellers

APIs for every shovel you need

Rent it; every rule update is billable.

"The banks panned for compliance. The vendors sold the pans."

Why Do Banks Now Rent Compliance from Third Parties Instead of Building It In-House?

The Make-or-Buy Shift
Every rule update — a new sanctions designation, a revised KYC tier, a fresh reporting taxonomy — forces banks to re-engineer internal systems. Each bank repeats identical work on slightly different stacks. RegTech vendors absorb that fixed-cost friction and sell it back as a shared subscription service.

- **Fragmented rules:** dozens of regulators, thousands of list updates, hundreds of reporting formats.
- **Fixed-cost problem:** each bank rebuilds the same rule parser, the same screening engine, the same dashboard.
- **Asymmetric outcome:** a small vendor that serves many banks amortises the fixed cost across all of them; a bank building alone pays the full cost alone.

The friction the RegTech BM exploits is not a customer friction — it is an **internal-operations friction**. The customer is not the end-user; the customer is the compliance team.

One vendor absorbs the fixed cost for many banks.

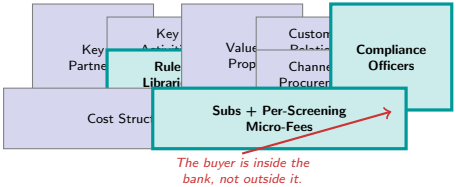
The RegTech BM monetises an internal friction: every bank re-implements the same rule engine. A vendor pools the fixed cost and sells access back as Software-as-a-Service (BMC Value Proposition block).

Which Canvas Blocks Make a Compliance Vendor Look Nothing Like a Consumer FinTech?

The B2B SaaS Canvas, Adapted
Osterwalder's Business Model Canvas frames nine interlocking blocks: value proposition, customer segments, channels, revenue streams, key resources, key activities, key partners, cost structure, customer relationships. For RegTech, three blocks re-define themselves away from the typical consumer-FinTech template.

- **Customer Segments:** compliance officers and risk teams inside financial institutions — never the end-user. The buyer signs procurement contracts, not app-store downloads.
- **Key Resources:** curated lists, rule libraries, and model validation evidence — regulatory-grade data, not UX polish.
- **Revenue Streams:** subscription tiers and per-screening micro-fees, bundled with professional-services onboarding.

(In business-model language, a *moat* = a competitive advantage that rivals cannot easily copy.)
The canvas reveals that RegTech is closer to an enterprise-software category than to a consumer-finance category. The moat is procurement lock-in plus evidence inventory, not network effects.



Osterwalder's Business Model Canvas adapted to RegTech: three blocks (Customer Segments, Key Resources, Revenue Streams) depart sharply from consumer-FinTech defaults.

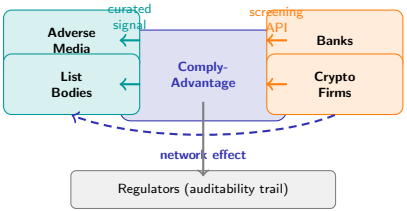
How Does ComplyAdvantage Turn a List-Screening API into a Two-Sided Data Platform?

Two-sided platform = a service that sells access to one user group by first attracting another. Value rises on both sides as each side grows.

The ComplyAdvantage Case (ComplyAdvantage, United Kingdom)

ComplyAdvantage, headquartered in London, sits between two populations: the data producers (adverse-media sources, list bodies, public filings) on one side, and the data consumers (financial institutions issuing screening queries) on the other. Each side makes the other more valuable.

- **Multi-sided platform:** more client screening volume sharpens the relevance signal on the data side; richer data makes the platform more attractive to new clients.
- **Cross-side network effect:** every new client query surfaces missing entities, which the vendor back-fills into the curated list; every new list entry raises detection recall for all existing clients.
- **Chicken-and-egg solution:** the vendor subsidised the data side first — ingesting and curating listings well before banks arrived — then marketed a richer data asset than any single bank could assemble alone.
- Invisible to end-users, indispensable to the compliance team.



Platform economics explains the moat: each new client makes the curated list sharper; each sharper list makes the platform indispensable. Network effects without consumer-facing surface area.

Which Adjacent Compliance Products Does Onfido Add After Its Identity Wedge, and In What Sequence?

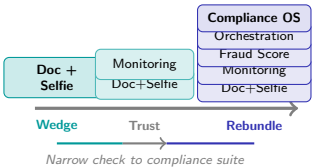
Unbundling = pulling one service out of a historical bundle and offering it alone; *rebundling* = stacking adjacent services onto that foothold once trust is established. Clayton Christensen (Harvard Business School) argued disruptors start narrow and cheap, earn trust, then expand upward.

Onfido's Rebundling Arc (Onfido, United Kingdom)

Onfido, headquartered in London, entered with a single wedge: automated document-plus-selfie identity verification. Christensen's disruption cycle predicts what happens next — the single-product vendor earns trust, then rebundles adjacent compliance products.

- **Wedge:** document and biometric identity capture at onboarding. Replaces in-branch paperwork with a phone camera.
- **First adjacency:** ongoing identity monitoring — re-verifying an existing customer when risk triggers fire.
- **Second adjacency:** fraud-signal scoring bundled into the verification call so every check carries a risk label.
- **Third adjacency:** orchestration — letting the client chain multiple checks (watchlist, proof-of-address, source-of-funds) behind one integration.

The irony: a company that launched to *unbundle* identity out of core banking software now rebundles it into a compliance suite that looks, functionally, like a miniature bank-ops stack.

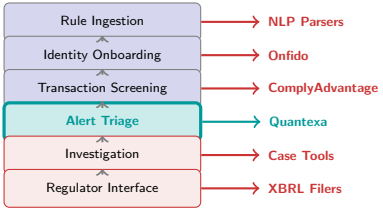


Christensen's unbundling-to-rebundling cycle: Onfido's wedge (identity check) earns procurement trust, after which adjacent products lower the marginal integration cost and raise switching costs inside the compliance team.

Where in the Compliance Value Chain Does Quantexa Insert Its Entity-Resolution Layer?

The Compliance Value Chain (Quantexa, United Kingdom)
Evans and Wurster argued that information-rich value chains will deconstruct — each link becomes separately contestable. Quantexa, headquartered in London, picks one link and dominates it. The compliance stack is textbook: six linked activities, each separately addressable.

- **Rule Ingestion** — parse new lists and rule texts.
- **Identity Onboarding** — KYC document and biometric capture.
- **Transaction Screening** — real-time checks against lists.
- **Alert Triage** — *Quantexa attacks here* — resolve scattered data points into a single entity view so an analyst sees one story, not a queue of fragments.
- **Investigation & Reporting** — case building and SAR drafting.
- **Regulator Interface** — XBRL filings, supervisory Q&A.



Quantexa does not try to own the whole chain. It owns the hardest link — entity resolution inside triage — and integrates above and below it. The link with the richest data advantage captures the largest slice of compliance spend.

Evans-Wurster value chain deconstruction: Quantexa claims the triage link because that is where the data-resolution moat lives. Adjacent links become integration surface, not competitive battlegrounds.

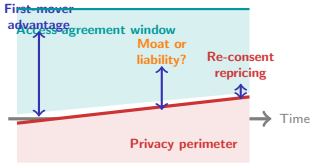
Is Trulioo's Cross-Border Data-Access Licence a Durable Moat or a Shrinking Arbitrage?

Regulatory arbitrage = a firm earns profit specifically because it faces a lighter rulebook than its competitors, not because it is better at the underlying business. The advantage lasts only as long as the rulebook gap does. A *moat* = a competitive advantage that rivals cannot easily copy.

The Arbitrage-to-Moat Question (Trulioo, Canada)

Trulioo, headquartered in Vancouver, rests its advantage on contractual data-access agreements with national bureaus, registries, and telco partners across many jurisdictions. No single bank — and few competitors — can replicate that agreement web cheaply.

- **Arbitrage variant:** the agreements exist in a grey space between privacy law, data-residency rules, and consent regimes that are still settling across jurisdictions.
- **Moat variant:** once agreements are signed and integrations audited, they are non-transferable and accumulate switching costs at the bureau side (not just the customer side).
- **Regulatory risk:** privacy-minimisation rules tightening in one jurisdiction can invalidate entire access channels — the moat becomes a liability overnight.



The canonical RegTech answer: convert arbitrage into regulatory capability. Sign the agreements early, audit them under supervisory eyes, and make compliance itself the barrier to entry for later competitors.

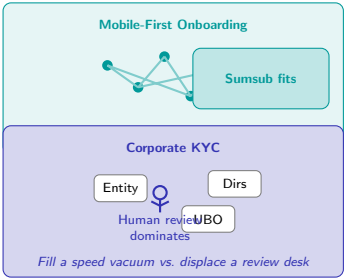
Regulatory arbitrage in RegTech flips into a compliance moat only when the vendor treats supervisory engagement as a core activity. Passive arbitrage erodes; actively documented access agreements compound.

Why Does Sumsub Thrive in Mobile-First Gig-Economy Markets but Stall in Branch-Heavy Corporate-Banking Ones?

The Context-Dependency Lesson (Sumsub, United Kingdom)
Sumsub, headquartered in London, sells mobile-first verification-as-a-service, a product that thrives in markets where the onboarding funnel must finish inside a phone session. Crypto exchanges, gig-economy platforms, and cross-border remittance apps lose customers with each friction step, so they pay for seconds-long verification.

- Mobile-first onboarding pipelines need **instant** verification, not three-day in-branch processes. Sumsub fills that vacuum where banks cannot.
- In corporate-banking onboarding, the legal entity, beneficial owners, and directors must be verified across jurisdictions. That process is slower, touches multiple human reviewers, and makes seconds-scale automation less valuable.
- The BM works where **speed** is a revenue lever. It stalls where **assurance** dominates and human review cannot be substituted out.

Context determines which RegTech BM wins: fill a speed vacuum in consumer-scale onboarding, or displace an incumbent inside a slow, human-heavy corporate workflow.



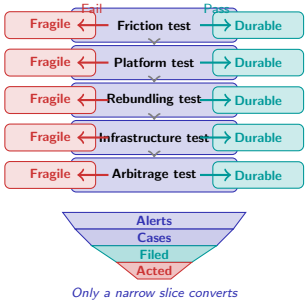
Sumsub's insight: where onboarding speed is itself a revenue lever, automation fills a vacuum. In corporate KYC, the human reviewer is the product; automation is a supporting tool.

Which Five Tests Separate a Shovel Seller That Outlasts the Rush from One That Vanishes With It?

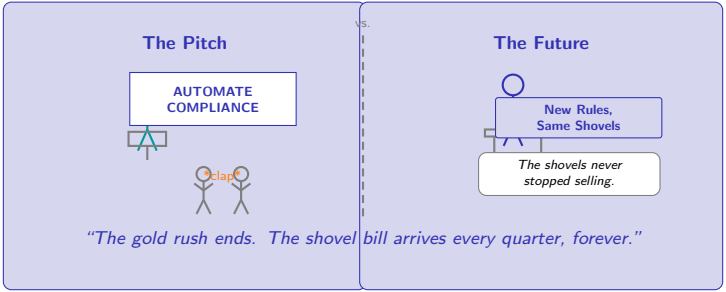
The Five-Test Synthesis for RegTech

1. **Friction test:** Does the vendor solve a real *internal* friction — a re-engineering cost every bank otherwise bears alone? Or does it merely re-skin an existing in-house tool?
2. **Platform test:** Does a two-sided flywheel exist between data producers and data consumers? Network effects in RegTech live on the data side, not the UX side.
3. **Rebundling test:** Can adjacent compliance products be added behind one integration? A single-check vendor is a feature; a compliance suite is a platform.
4. **Infrastructure test:** Is the vendor filling a vacuum (mobile-first onboarding) or displacing a human review desk (corporate KYC)? Filling is easier.
5. **Arbitrage test:** Is the advantage a shrinking privacy-or-consent gap — or a documented supervisory moat that later entrants cannot replicate cheaply?

Durable shovel sellers pass at least three tests. A pure technology wedge — no data moat, no rebundling, no supervisory depth — dies with the rush it served.



Durable RegTech shovel sellers pass at least three tests. The funnel itself is the product: converting a mountain of alerts into a narrow stream of regulator-ready actions.



"The gold rush ends. The shovel bill arrives every quarter, forever."