

Fintech Security and Regulation

Navigating Compliance in the Digital Finance Era

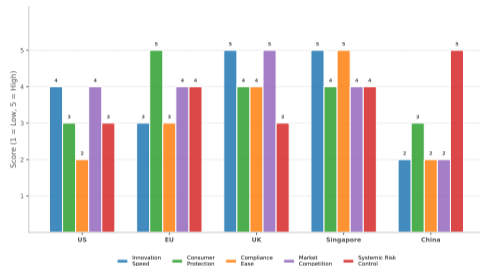
Bridge from Lecture 3

In Lecture 3 we explored the mechanics of **payment systems**: card networks, real-time rails, interchange economics, and regulation like Durbin and PSD2.

Now we zoom out to the full **regulatory landscape** surrounding fintech:

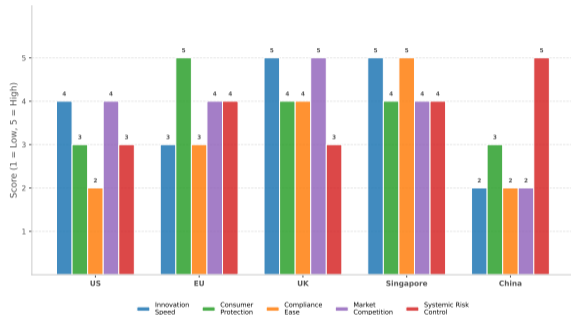
- **Payments regulation** was just one piece — fintech firms face anti-money laundering (AML), know-your-customer (KYC), data protection, and licensing requirements simultaneously.
- **Security is existential**: A single breach can destroy consumer trust built over years. Regulation exists to enforce minimum security standards.

Regulatory Approaches: Cross-Country Comparison



Regulatory Approaches to Fintech

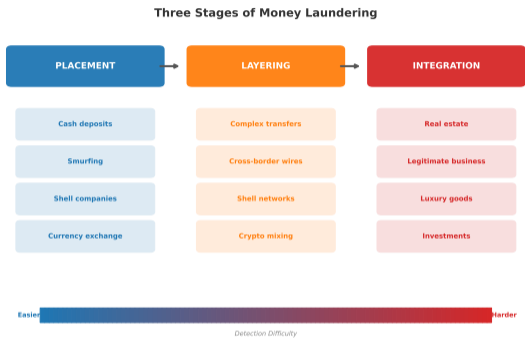
Regulatory Approaches: Cross-Country Comparison



Jurisdictions adopt fundamentally different philosophies:

- **Activity-based** (UK, Singapore) — Regulate what a firm *does*, not what it *is*. Enables innovation but creates gaps when activities span categories.
- **Entity-based** (USA) — Regulate based on charter type (bank, broker-dealer, MSB). Clear boundaries but fintechs struggle to fit legacy categories.
- **Sandbox-first** (UK FCA, MAS, Abu Dhabi) — Allow controlled experimentation with reduced requirements. Time-limited, small scale, supervised.

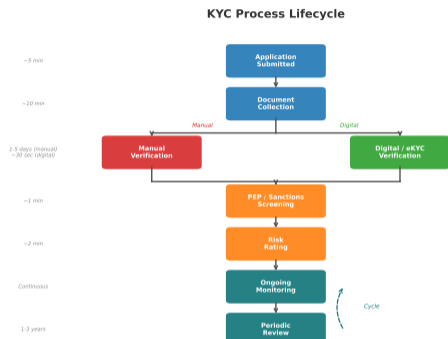
Money Laundering: The Three Stages



All money laundering follows the same three-stage pattern:

- 1 **Placement** — Introducing illicit cash into the financial system. Methods: structuring deposits below reporting thresholds (“smurfing”), cash-intensive businesses, prepaid cards.
- 2 **Layering** — Creating complex transaction chains to obscure the money trail. Shell companies, cross-border transfers, cryptocurrency mixing, trade-based laundering.
- 3 **Integration** — Re-introducing “clean” money into the legitimate economy. Real estate, luxury goods, business

Know Your Customer (KYC)

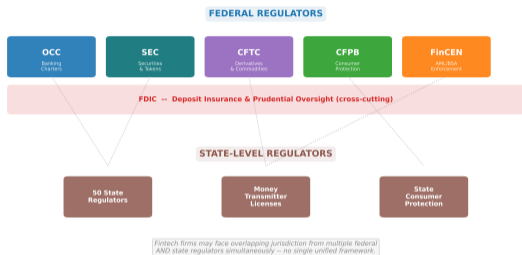


KYC is the first line of defense against financial crime:

- **Customer Identification Program (CIP)** — Verify identity at onboarding: government ID, biometric checks, address verification, liveness detection.
- **Customer Due Diligence (CDD)** — Assess risk profile: source of funds, expected transaction patterns, PEP (Politically Exposed Person) screening.
- **Enhanced Due Diligence (EDD)** — For high-risk customers: deeper investigation, senior management approval, ongoing monitoring with tighter thresholds.

The US Regulatory Patchwork

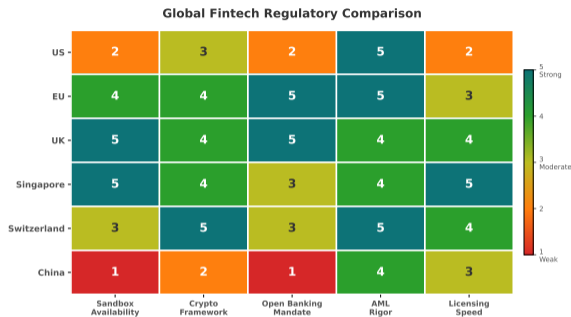
US Fintech Regulatory Landscape: The Patchwork Problem



The United States has no single fintech regulator — instead, a fragmented system of overlapping authorities:

- **Federal:** OCC (banks), SEC (securities), CFTC (derivatives), FinCEN (AML/KYC), CFPB (consumer protection), Federal Reserve (systemic risk).
- **State:** 50 separate money transmitter licenses (MTLs). A payments startup must apply individually in each state — costing \$1–5M and 12–24 months.
- **Gaps:** Crypto assets may fall under SEC, CFTC, state regulators, or none depending on classification.

Global Regulatory Comparison



Illustrative scores (1 = Weak/Absent, 5 = Strong/Comprehensive)

Regulatory maturity varies dramatically across jurisdictions:

- **EU:** MiCA (2024) creates unified crypto-asset regulation. PSD2/PSD3 for payments. GDPR for data. DORA (2025) for digital operational resilience.
- **UK:** FCA sandbox model. Activity-based licensing. Post-Brexit divergence creating regulatory competition with EU.
- **Singapore:** MAS Payment Services Act (2020). Licensing tiers based on transaction volume. Highly regarded sandbox.

RegTech: Technology Stack

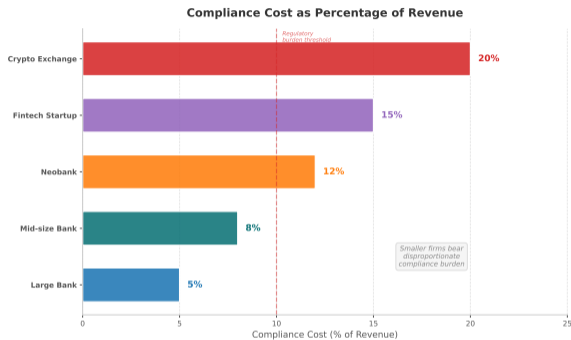
RegTech Technology Stack



RegTech uses fintech's own tools to solve the compliance burden:

- **Identity layer:** Biometric verification, document authentication, liveness detection — enabling eKYC in under 60 seconds.
- **Transaction monitoring:** Real-time rule engines plus ML-based anomaly detection. Reduces false positives from 95%+ (legacy) to 50–70%.
- **Regulatory reporting:** Automated generation of SAR, CTR, and prudential reports. Machine-readable regulation (XBRL, RegML) enables straight through processing.

The Compliance Cost Burden



Compliance is one of the largest operating costs for financial firms:

- **Global banks** spend 5–10% of revenue on compliance, totaling over \$270B annually across the industry.
- **Fintechs** face disproportionate burden: compliance costs are largely fixed, so they consume 15–25% of revenue for early-stage firms vs. 3–5% for large banks.
- **AML fines** exceeded \$5B globally in 2023. A single enforcement action can be existential for a fintech (Wirecard: fraud, not just non-compliance).

Core Concepts:

- 1 **Regulation is not monolithic** — approaches range from activity-based to entity-based, sandbox to prohibition. No single model dominates globally.
- 2 **AML/KYC is the universal requirement** — every fintech touching money must implement placement, layering, and integration detection. The cost is non-trivial.
- 3 **The US patchwork is uniquely burdensome** — 50-state licensing plus overlapping federal agencies creates high barriers and regulatory arbitrage incentives.

Looking Ahead to Lecture 5:

With payment mechanics (L03) and the regulatory landscape (L04) established, Lecture 5 will explore **blockchain and decentralized finance (DeFi)** — technologies that attempt to bypass traditional intermediaries and regulators entirely.

Questions to carry forward:

- Can decentralized protocols comply with AML/KYC requirements designed for centralized institutions?
- Does “code is law” replace or complement legal regulation?