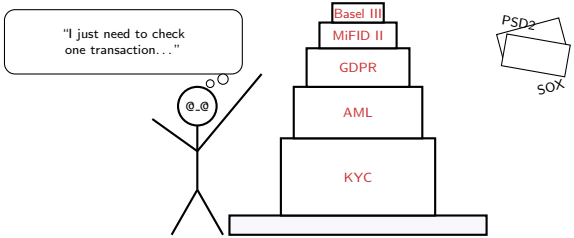
RegTech & Compliance

Lesson 04

Digital Finance



After 2008, the rules multiplied — but the tools didn't.

Outline

Learning Objectives

By the end of this lesson, you will be able to:

1. Explain why financial regulation exists using market failure theory
2. Define **RegTech** and classify its major solution categories
3. Describe **KYC** and **AML** processes as regulatory responses to information asymmetry
4. Analyze how technology automates compliance workflows and reduces costs
5. Evaluate the principal-agent relationship between regulators, banks, and customers

---

This lesson connects regulatory economics (market failures, agency problems) to practical compliance technology.

Why Can't We Just Let Financial Markets Regulate Themselves?

Banks are private companies that should be free to take risks and innovate. But when Lehman Brothers failed, the entire global economy suffered — because bank failures create costs that banks don't pay.

Four market failures justify financial regulation:

1. **Externalities:** A bank failure harms the entire economy through credit contraction, job losses, and lost savings – costs the failing bank does not internalize
2. **Information asymmetry:** Banks know more about their risk than customers or regulators (recall Lessons 01 & 03: adverse selection and moral hazard)
3. **Moral hazard from deposit insurance:** When deposits are insured, banks take excessive risks because they don't bear the full downside (government bears it)
4. **Public goods:** Financial stability benefits everyone (non-excludable, non-rivalrous) but individual banks have no incentive to provide it

Economic logic: Without regulation, competitive pressures push banks toward socially excessive risk-taking.

Without regulation, individual banks would take excessive risks because they don't bear the full cost of failure.

What Happens When a Bank Is Too Big to Fail?

Systemic risk is the risk that failure of one institution triggers a cascade of failures throughout the financial system.

Too Big to Fail (TBTF):

- When a financial institution is so large or interconnected that its failure would cause catastrophic economic damage
- Creates **moral hazard**: TBTF institutions believe they have an implicit government guarantee
- They take on excessive risk (higher leverage, riskier assets) knowing they will be bailed out
- Smaller institutions bear the full cost of failure; TBTF institutions externalize it to taxpayers

The 2008 Global Financial Crisis:

- Lehman Brothers (NOT bailed out) triggered a cascade: AIG, Merrill Lynch, Citigroup, others required rescue
- Demonstrated that systemic risk was drastically underestimated by both banks and regulators
- Led to massive regulatory expansion (Dodd-Frank in US, Basel III globally – see Lesson 07)

The 2008 crisis showed that systemic risk was drastically underestimated by both banks and regulators.

Who Watches the Watchmen in Financial Regulation?

Multiple layers of principal-agent relationships in finance:

Principal	Agent	Conflict / Information Problem
Depositors / customers	Bank management	Customers don't observe bank risk-taking Management maximizes profit, not customer safety
Public / taxpayers	Regulators	Regulators may be "captured" by industry (Lesson 02) Voters don't observe regulator effort or quality
Shareholders	Bank management	Management may take excessive risk (upside to them, downside to shareholders and depositors)

How compliance addresses agency problems:

- **Mandatory disclosure** reduces information asymmetry between banks and regulators
- **KYC/AML** reduces information asymmetry between banks and customers
- **Capital requirements** align bank incentives with depositor safety (Lesson 07)

Understanding these agency relationships explains why compliance is costly but necessary.

Why Did Compliance Costs Explode After 2008?

After 2008, regulators wrote thousands of pages of new rules. Major banks now employ 10,000+ compliance staff each. The rules multiplied, but the tools stayed in the 1990s.

Definition: RegTech (Regulatory Technology) is the use of technology to manage regulatory processes within the financial industry more effectively and efficiently.

Why RegTech emerged:

- Post-2008 regulatory expansion (Dodd-Frank, MiFID II, Basel III, GDPR) massively increased compliance costs
- Banks spent billions on compliance – by 2020, major banks had 10,000+ compliance staff each
- Manual compliance processes are slow, error-prone, and expensive
- **Economic logic:** Regulation creates transaction costs; technology reduces transaction costs

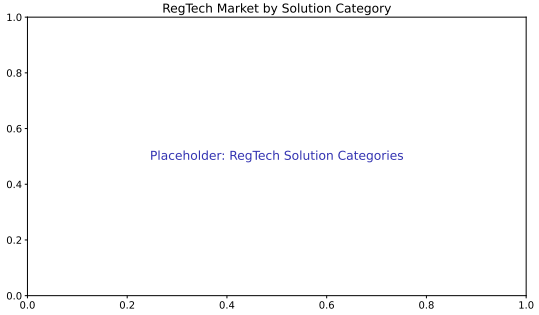
Key insight: RegTech is to compliance what FinTech is to banking – using technology to reduce the friction (transaction costs) of a necessary but expensive activity.

Core technologies: Machine learning (ML), natural language processing (NLP), robotic process automation (RPA), blockchain, cloud computing, APIs

---

RegTech is to compliance what FinTech is to banking – technology reducing transaction costs.

Which Regulatory Problem Does Each RegTech Category Solve?



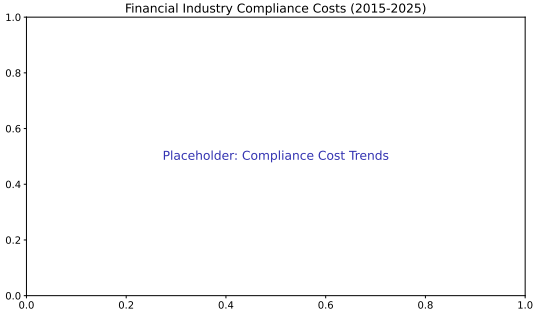
Each category addresses a regulatory problem:

- **Identity & KYC:** Customer identity asymmetry
- **Transaction & AML:** Detect illegal activity
- **Risk management:** Measure/report risks
- **Reporting:** Reduce regulator asymmetry
- **Automation:** Reduce adherence costs

Key: RegTech reduces *cost* of compliance.

Each RegTech category addresses a specific information or monitoring problem.

How Did Compliance Costs Grow Faster than Bank Revenue?



Post-2008 cost drivers:

- Complexity (Dodd-Frank: 400+ rules)
- Multi-jurisdiction (US, EU, Asia)
- Massive fines (HSBC $1.9bn, JPM $2.6bn)
- Talent shortage

RegTech value:

- Automate collection/checking
- Reduce false positives
- Faster, accurate reporting
- Scalable without cost growth

Compliance costs have grown faster than bank revenues – making RegTech necessary.

Why Must Your Bank Know So Much About You?

A new customer walks into a bank. They could be anyone: a teacher, a CEO, or a money launderer. The bank must figure out which one — and the consequences of getting it wrong include billion-dollar fines.

KYC is the process of verifying customer identity and assessing risk to prevent fraud, money laundering, and terrorist financing.

Economic foundation: KYC addresses **information asymmetry** – the bank knows less about the customer than the customer knows about themselves (especially their intentions).

Three pillars of KYC:

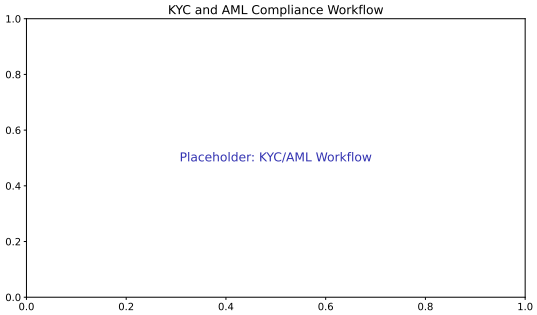
1. **Customer Identification Program (CIP):** Collect name, address, date of birth, ID number – verify against government-issued documents
2. **Customer Due Diligence (CDD):** Assess customer risk based on occupation, source of funds, expected transaction patterns
3. **Enhanced Due Diligence (EDD):** Additional scrutiny for high-risk customers (politically exposed persons, high-net-worth individuals, customers from high-risk jurisdictions)

When KYC applies: Account opening, large transactions, suspicious activity, periodic reviews

---

KYC is fundamentally about reducing the information asymmetry between a bank and its customer.

How Does Each KYC Step Reduce the Bank's Uncertainty?



Information economics of each step:

- **Data collection:** Reduces uncertainty about customer identity
- **Verification:** Confirms claims (reduces adverse selection)
- **Risk assessment:** Uses observable characteristics to infer unobservable risk
- **Ongoing monitoring:** Detects behavior changes (moral hazard)
- **Alert investigation:** Human judgment on illegal activity
- **SAR filing:** Reports suspicion to government to reduce information asymmetry

Each step reduces the bank's uncertainty about customer identity and intent.

How Do Criminals Make Dirty Money Look Clean?

Money laundering is the process of making illegally obtained money appear legitimate.

Three stages of money laundering:

1. **Placement:** Introduce illegal cash into the financial system (e.g., deposit $9,000 repeatedly to avoid $10,000 reporting threshold – called "structuring")
2. **Layering:** Move money through complex transactions to obscure its origin (wire transfers, shell companies, cross-border flows)
3. **Integration:** Use now-"clean" money for legitimate purchases (real estate, businesses, luxury goods)

AML as extreme information asymmetry: Money launderers deliberately hide the true source and purpose of funds. Banks must detect this hidden information.

Global AML framework:

- **FATF** (Financial Action Task Force) sets international standards
- **SARs** (Suspicious Activity Reports): banks file with government when they detect potential money laundering
- Estimated 2-5% of global GDP ($1-2 trillion) is laundered annually

---

Money laundering is estimated at 2-5% of global GDP – trillions of dollars annually.

Can AI Reduce the 95% False Positive Rate in Transaction Monitoring?

How technology transforms KYC/AML:

Process	Traditional (Manual)	RegTech Solution
Identity verification	Examine documents in branch	Digital ID verification (OCR, biometrics, liveness detection)
Risk assessment	Analyst reviews forms, scores manually	AI-driven risk scoring using hundreds of variables
Transaction monitoring	Rule-based alerts (e.g., amount $>$ \$10k) $\rightarrow$ 95%+ false positives	ML models detect anomalies (e.g., sudden geographic change) $\rightarrow$ reduces false positives to manageable levels
Watchlist screening	Manual name matching against sanctions lists	Fuzzy matching, NLP for name variants, real-time API checks

Examples: Onfido (digital identity verification), **ComplyAdvantage** (AML data and screening)

Technology reduces false positives from over 95% to manageable levels – saving thousands of analyst hours.

What Can Automation Handle – and What Still Needs Human Judgment?

A compliance officer reviews 500 transaction alerts per day. 95% are false positives. They spend 8 hours finding 25 real cases.

Comparison: Manual vs. automated compliance

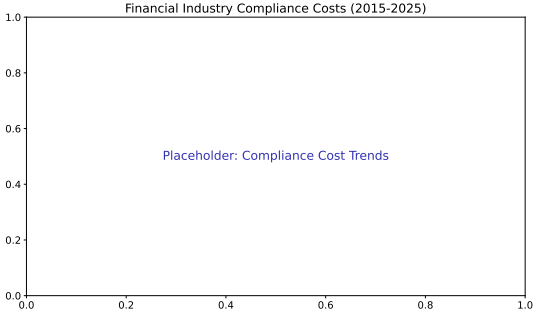
Compliance Activity	Manual	Automated (RegTech)
Data collection	Employees gather data from multiple systems, export to Excel	APIs pull data from source systems automatically (real-time or scheduled)
Rule checking	Compliance officer reads rule text, manually checks if activity complies	Rules codified in logic; system checks data against rules; flags exceptions
Report generation	Analyst compiles data, formats, manually submits to regulator	System auto-generates reports in required format, submits via regulator API
Alert triage	Analyst reviews EVERY alert (95%+ false positives)	ML ranks alerts by risk; analyst reviews only high-priority alerts

Key technologies:

- **NLP** (Natural Language Processing): Reads and interprets regulatory text (e.g., new rules) and contracts
- **RPA** (Robotic Process Automation): Automates repetitive tasks (data entry, form filling, report generation)

Automation does not replace compliance officers – it frees them to focus on complex judgments.

Why Do Costs Keep Rising Despite RegTech?



Why costs rise despite RegTech:

- Scope expanding (GDPR, MiFID II, crypto)
- Manual processes still common
- Upfront investment needed

ROI case:

- Reduced false positives: 1000s hours saved
- Faster: minutes vs. days onboarding
- Fewer fines via automation
- Scalability: 10x volume, same team

Evidence: 30-50% cost reduction.

The ROI case: reduced false positives, faster processing, fewer fines.

What Do Regulators Actually Need to See – and Why?

Regulators can't sit inside every bank and watch what happens. Mandatory reporting is how regulators see through the information asymmetry — but the reports themselves are expensive to produce.

What regulators require from banks:

- **Capital and liquidity reports:** Basel III requires detailed reports on risk-weighted assets, liquidity coverage ratio (LCR), net stable funding ratio (NSFR) – see Lesson 07
- **Transaction reports:** MiFID II (EU) requires reporting of every securities transaction
- **Conduct and compliance reports:** Quarterly or annual attestations that bank complies with consumer protection, AML, etc.
- **Stress test submissions:** Banks submit data to regulators who run macroeconomic stress scenarios

Reporting as a monitoring mechanism: Regulators cannot observe bank behavior directly (information asymmetry). Mandatory reporting reduces this asymmetry.

Data standards:

- **XBRL** (eXtensible Business Reporting Language): Standardized format for financial data
- **ISO 20022**: Global standard for electronic data interchange in financial services

Data quality is critical: Errors in reporting can trigger investigations and fines.

Regulatory reporting is the mechanism through which regulators reduce their own information asymmetry.

How Are Regulators Using the Same Technology as Banks?

SupTech (Supervisory Technology) is the use of technology by regulatory authorities to enhance supervision and surveillance.

How SupTech works:

- **Real-time surveillance:** Regulators receive data feeds from banks (via APIs) and monitor in real-time (instead of quarterly reports)
- **Automated data collection:** Machine-readable regulatory submissions reduce manual data entry errors
- **ML for risk detection:** Regulators use ML to identify banks with high risk profiles for deeper investigation
- **Data pooling:** Aggregate data across institutions to detect systemic risks

Examples:

- **Bank of England:** Uses ML to analyze bank stress test submissions
- **Monetary Authority of Singapore (MAS):** COSMIC platform for regulatory data collection and analytics

Economic insight: SupTech mirrors RegTech – both sides of the principal-agent relationship (banks and regulators) adopt technology to reduce information asymmetry and transaction costs.

SupTech mirrors RegTech – both sides of the principal-agent relationship adopt technology.

What Blocks Banks from Adopting RegTech?

Common obstacles:

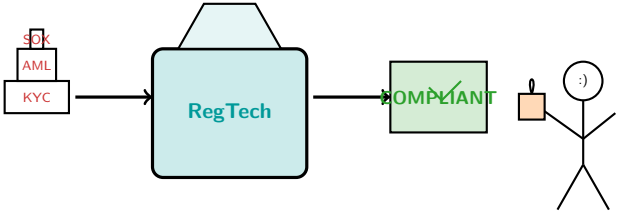
1. **Legacy system integration:** Banks have decades-old core systems; RegTech solutions must integrate with them (costly, time-consuming)
2. **Data silos:** Customer data, transaction data, risk data often in separate systems that don't communicate
3. **Change resistance:** Compliance officers fear job loss; IT departments resist new technology
4. **Vendor lock-in:** Proprietary RegTech solutions make it hard to switch providers
5. **Regulatory uncertainty:** Regulators slow to approve new compliance technologies (prefer proven methods)

Best practices:

- Start with a pilot: Prove ROI in one area before scaling (e.g., automate AML for retail banking before investment banking)
- Build vs. buy: Large banks build custom solutions; smaller banks buy off-the-shelf RegTech
- API-first architecture: Use open APIs to avoid vendor lock-in and enable integration

Swiss examples: NetGuardians (AI-based fraud detection), **Apiax** (regulatory content as a service)

Start with the highest-cost compliance area to demonstrate ROI before broader rollout.



Technology doesn't remove the rules — it makes following them possible.

Summary

Key takeaways from Lesson 04:

1. **Regulation exists because of market failures:** Externalities (bank failures harm economy), information asymmetry, moral hazard (TBTF), and public goods (financial stability). Compliance aligns bank incentives with social welfare.
2. **RegTech reduces compliance costs, not regulatory burden:** Post-2008 regulatory expansion made compliance prohibitively expensive. RegTech uses ML, NLP, RPA to automate workflows, reduce false positives, and scale compliance operations.
3. **KYC and AML address information asymmetry:** Banks must verify customer identity (KYC) and detect hidden illegal activity (AML). Technology (digital ID, ML-based transaction monitoring) makes this faster and more accurate.
4. **SupTech mirrors RegTech:** Regulators also use technology (real-time data feeds, ML for risk detection) to reduce their information asymmetry about bank behavior. This creates a technology-driven compliance ecosystem.

Connection to future lessons: Lesson 05 (Blockchain) introduces a technology that proposes to solve the trust problem without intermediaries.

Next lesson: Blockchain Fundamentals – a technology that proposes to solve the trust problem without intermediaries.