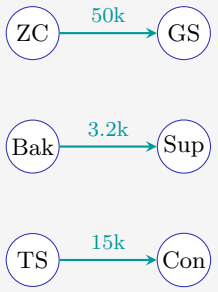
Pre-Class Discovery Handout: RegTech & Compliance

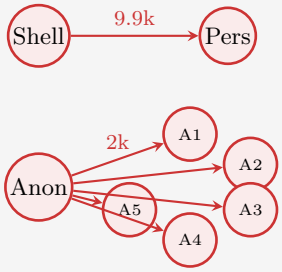
Activity 1: Follow the Money

Scenario: You are an AML analyst reviewing five transactions flagged by your monitoring system. Study the transaction table and network diagram, then identify the suspicious activity.

#	From	To	Amount (CHF)	Pattern
1	Zurich Corp	Geneva SA	50,000	Regular monthly
2	Shell Co (Cayman)	Personal Acct	9,900	Just under threshold
3	Bakery	Supplier	3,200	Regular
4	Anonymous	5 accounts	2,000 each	Same day
5	Tech Startup	Contractor	15,000	Invoice attached



Normal flows



Suspicious flows

Q1: Which transactions are suspicious? Identify the specific AML red flags for each.

Q2: What additional information would you request to investigate each suspicious transaction?

Q3: Why is transaction #2 particularly concerning? (Hint: structuring / smurfing.)

Activity 2: The False Positive Dilemma

Scenario: A bank's transaction monitoring system flags 1,000 transactions per day. Of these, 95% are false positives. Each manual investigation costs CHF 100.

Q1: Calculate the daily investigation cost under the current system.

Q2: If an AI-based system reduces false positives to 50%, what is the new daily cost? How much money is saved per day?

Q3: If AI further reduces false positives to only 10%, is the cost problem solved? What is the dangerous tradeoff with false negatives?

Activity 3: RegTech Solution Matching

Scenario: Match each regulatory requirement to the RegTech solution category that addresses it.

Regulatory Requirement	RegTech Solution
KYC identity verification	
AML transaction monitoring	
Regulatory reporting	
Risk assessment	
Data privacy / GDPR	

Solution categories: Biometric ID verification, Pattern-detection AI, Automated report generation, Predictive analytics, Privacy-enhancing technologies.

Q1: Match each requirement to the most appropriate solution category from the list above.

Q2: Which regulatory requirement is the hardest to fully automate? Explain why in 2–3 sentences.

Solutions

Activity 1: Follow the Money

A1: Transactions **#2** and **#4** are suspicious. #2 red flags: the amount (CHF 9,900) is deliberately just below the CHF 10,000 reporting threshold, the sender is a shell company in a secrecy jurisdiction (Cayman Islands), and the recipient is a personal account. #4 red flags: an anonymous source distributes identical amounts to five accounts on the same day—a classic layering/structuring pattern.

A2: For #2: request beneficial ownership records for the Cayman shell company, source-of-funds documentation, and the relationship between the shell company and the personal account holder. For #4: request identification of the "anonymous" sender, the relationship between all five receiving accounts, and whether the accounts share any common characteristics (address, IP, phone number).

A3: Transaction #2 is structuring ("smurfing")—deliberately keeping amounts below the mandatory reporting threshold (CHF 10,000 in Switzerland) to avoid triggering a Suspicious Activity Report. This is a criminal offence in most jurisdictions even if the underlying funds are legitimate, because it constitutes deliberate evasion of AML controls.

Activity 2: The False Positive Dilemma

A1: Daily flags: 1,000. At CHF 100 per investigation: $1{,}000 \times$ CHF 100 = **CHF 100,000** per day. With 95% false positives, only 50 of those 1,000 are genuine—yet the bank must investigate all of them.

A2: At 50% false positives the system flags 50 true + 50 false = 100 total flags (assuming true positives remain constant, but total flags drop because the AI is more precise). More precisely, if 50 true positives remain and the false-positive rate is 50%, total flags $= 50/0.50 = 100$. Cost: $100 \times$ CHF 100 = CHF 10,000/day. Savings: CHF 90,000/day.

A3: At 10% false positives: total flags ≈ 56, cost $\approx$ CHF 5,600/day. The cost problem is largely solved, but the dangerous tradeoff is false negatives: if the AI is too aggressive in suppressing alerts, it may miss genuine money laundering (true suspicious transactions that go unflagged). A single missed case can result in regulatory fines, criminal liability, and reputational damage far exceeding the investigation savings.

Activity 3: RegTech Solution Matching

A1: KYC identity verification → **Biometric ID verification** (facial recognition, liveness detection). AML transaction monitoring → **Pattern-detection AI** (anomaly detection on transaction graphs). Regulatory reporting → **Automated report generation** (structured data extraction and submission). Risk assessment → **Predictive analytics** (ML models for credit, market, and operational risk). Data privacy / GDPR → **Privacy-enhancing technologies** (differential privacy, homomorphic encryption, secure enclaves).

A2: Risk assessment is the hardest to fully automate. Risk models must capture tail events (rare but catastrophic scenarios) that have few or no historical precedents, requiring human judgment about model assumptions. Additionally, risk assessment involves qualitative factors—management quality, geopolitical context, regulatory change—that resist quantification, and regulators require human accountability for risk decisions.

