CHARTA LEARNING · LESSON NOTES

Financial Crime and Fraud

FRM Part II

1 A story: two problems at Kestrel Bank

- A payments clerk pays his own fake supplier for a year
- A customer runs criminal cash through business accounts
- The first is fraud: the bank itself is deceived
- The second is laundering: the bank is used as a channel
- One framework must manage both risks

IN THE LESSON

- Picture Kestrel Bank, a mid sized lender.
- In the same year it finds two problems.
- A payments clerk has been paying a fake supplier, a company the clerk set up himself, for more than a year.
- And a customer has been running criminal cash through a string of business accounts.
- These are different crimes.
- In the first, the bank itself is deceived and loses money.
- That is fraud.
- In the second, the bank may lose nothing at first, but it is being used as a channel to hide where money came from.
- That is money laundering.
- Yet both pass through the same systems, the same staff and the same weak spots.
- So the bank needs one control framework that manages both risks, and building that framework is the first half of this lesson.

2 Two related risks, side by side

Related, but not the same crime

Question	Fraud	Money laundering
What is it?	Deception for gain	Disguising criminal proceeds
Harmed first	Bank or its customers	Society; bank's standing
Explained by	The fraud triangle	Three stages
Main controls	Remove opportunity	The AML programme

IN THE LESSON

- Let us set the two risks side by side, one row at a time.
- First, what is it?
- Fraud is deception for gain: someone lies, hides or falsifies records to take money or another benefit.
- Money laundering is disguising criminal proceeds, so that money from crime appears to come from a lawful source.
- Second, who is harmed first?
- In a fraud, the bank or its customers lose money directly.
- In laundering, the first harm falls on society, because crime is made to pay, and the bank's standing suffers when it is found to have carried the money.
- Third, what explains it?
- Fraud is usually explained by the fraud triangle.
- Laundering moves through three stages.
- Fourth, the main controls.
- For fraud, controls mainly remove opportunity.
- For laundering, the answer is the anti money laundering programme, which we will call the A M L programme.

3 The fraud triangle

Fraud usually needs all three sides; a bank's controls work mainly on one

Side	Meaning	Kestrel's clerk
Pressure	A need or motive	Gambling debts
Opportunity	A way to do it unseen	Sets up and pays suppliers
Rationalisation	A story that excuses it	Only borrowing it

IN THE LESSON

- Why do people commit fraud?
- The standard explanation is the fraud triangle.
- It has three sides, and a fraud usually needs all three.
- Pressure is a need or motive, often financial.
- Kestrel's clerk had gambling debts.
- Opportunity is a way to commit the fraud and keep it hidden.
- The clerk could both set up new suppliers and pay them, with nobody checking his work.
- Rationalisation is the story a person tells themselves to excuse the act.
- The clerk told himself that he was only borrowing, and would pay it back before anyone noticed.
- Now ask which side a bank can actually change.
- It has little control over a person's private pressures, and it cannot see inside their head.
- But it can design its processes so that the opportunity is small.
- That is why fraud controls focus mainly on opportunity.

4 Controls that remove opportunity

Each control makes it harder to act alone and stay hidden

Control	How it removes opportunity
Segregation of duties	Split set up, pay and check
Authorisation limits	Big payments need a 2nd approver
Mandatory leave	Someone else does the job
Reconciliations	Match records to outside data
Whistleblowing channel	Staff report concerns safely

IN THE LESSON

- Here are the five classic controls, and how each removes opportunity.
- Segregation of duties means splitting a task so that no one person runs it from end to end.
- The person who sets up a supplier should not be the person who pays it, and neither should check the result.
- Authorisation limits mean that a payment above a set size needs a second person to approve it.
- Mandatory leave means staff must take a block of holiday, so that someone else does the job for a while.
- Many frauds need daily attention to stay hidden, and they surface when the fraudster is away.
- Reconciliations match the bank's own records against an independent source, such as a bank statement or a counterparty's confirmation.
- And a whistleblowing channel lets staff report concerns safely, without fear of retaliation.

5 Example 1: getting under the limit

One signature up to $50,000; above that, two. The clerk wants to pay $180,000

Payment to the fake supplier	set up by the clerk	**$180,000**
Single-signature limit	above it: two signatures	**$50,000**
Split into four payments	180,000 ÷ 4	**$45,000 each**
Each payment against the limit	45,000 < 50,000	**passes**
Weekly same-payee total	4 × 45,000	**$180,000: flag**

IN THE LESSON

- Let us see how the clerk beat one control.
- At Kestrel, a single signature can approve a payment up to fifty thousand dollars, and above that a second approver must sign.
- The clerk wants to pay his fake supplier one hundred and eighty thousand dollars.
- That one payment would go to a second approver, so he splits it.
- One hundred and eighty thousand divided by four is forty five thousand dollars each.
- Each payment of forty five thousand is below the limit of fifty thousand, so each one passes with his own signature.
- The fix is a detective check.
- A weekly report that adds up all payments to the same payee shows a total of one hundred and eighty thousand dollars, and flags it.
- Splitting a payment to stay under a limit is a classic warning sign.

6 Example 2: what mandatory leave reveals

The clerk hides $15,000 a month in a suspense account he reconciles himself

Hidden each month	rolled forward each month	**$15,000**
Months undetected	he never takes leave	**14**
Total hidden	15,000 × 14	**$210,000**
Mandatory leave enforced	a colleague reconciles	**2 weeks**
Unexplained difference found	the reconciliation breaks	**$210,000**

Lesson: one person both doing and checking the work is an open door

IN THE LESSON

- A second scheme shows why mandatory leave and reconciliations work together.
- The clerk also hides fifteen thousand dollars a month in a suspense account, which is a holding account for items not yet sorted.
- The trick works because the clerk performs that account's reconciliation himself, and each month he rolls the unexplained item forward.
- That is a failure of segregation of duties.
- He never takes a holiday, and the scheme runs for fourteen months.
- Fifteen thousand times fourteen is two hundred and ten thousand dollars hidden.
- Then Kestrel enforces its rule of two consecutive weeks of mandatory leave.
- A colleague performs the reconciliation, and finds an unexplained difference of two hundred and ten thousand dollars.
- The lesson is that one person both doing and checking the work is an open door.

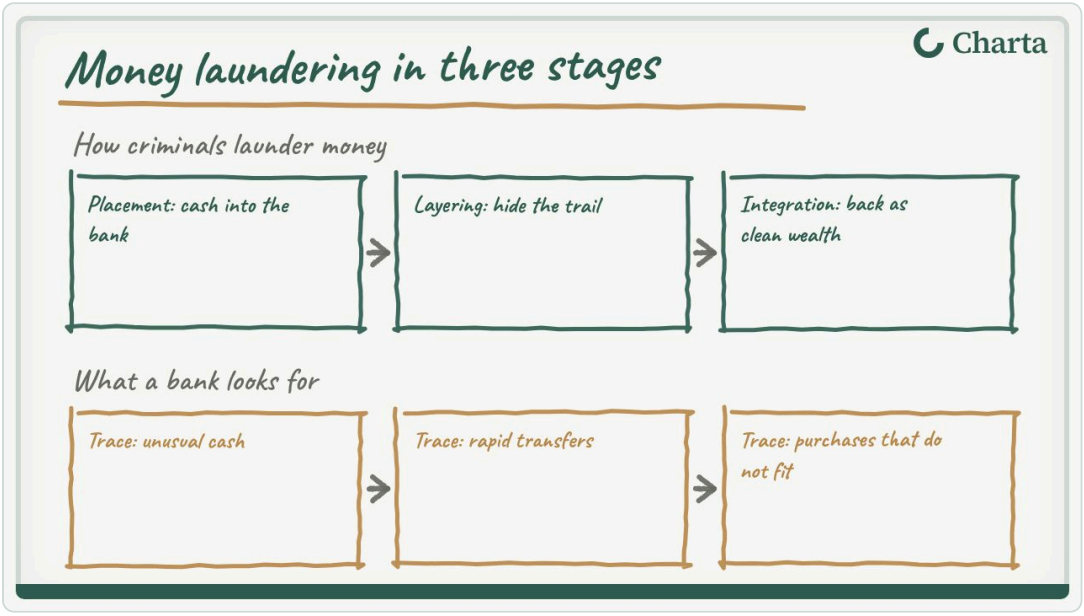
7 The exam trap: collusion

- Segregation of duties assumes people act alone
- Collusion: two or more people act together
- Then every check is signed by a partner in the scheme
- Back-ups: leave, outside reconciliations, whistleblowing
- Exam: collusion defeats segregation of duties

IN THE LESSON

- Now the exam point on fraud.
- Segregation of duties rests on an assumption: that the people in the chain act independently.
- Collusion breaks that assumption.
- Collusion means two or more people acting together, for example two staff, or a member of staff and an outsider such as a supplier.
- If the person who sets up a supplier and the person who approves the payment are in the scheme together, every check is signed by a partner in the fraud, and segregation of duties gives no protection at all.
- So a bank backs it up with controls that collusion finds harder to hide from: mandatory leave, reconciliations against outside data, and the whistleblowing channel.
- Remember the phrase for the exam: collusion defeats segregation of duties.

8 Money laundering in three stages



IN THE LESSON

- Now the second risk.
- Money laundering moves criminal proceeds through three stages.
- Look at the top row, which shows how criminals launder money.
- Placement is getting the cash into the financial system, for example by depositing it in a bank account.
- Layering is moving the money around, often many times and across accounts, products and countries, so that the trail back to the crime becomes hard to follow.
- Integration is bringing the money back into the lawful economy as apparently clean wealth, for example by buying property or investing in a business.
- The point for a risk manager is in the second row, what a bank looks for.
- Each stage leaves a different trace: unusual cash at placement, rapid transfers at layering, and purchases that do not fit the customer at integration.

9 What each stage looked like at Kestrel

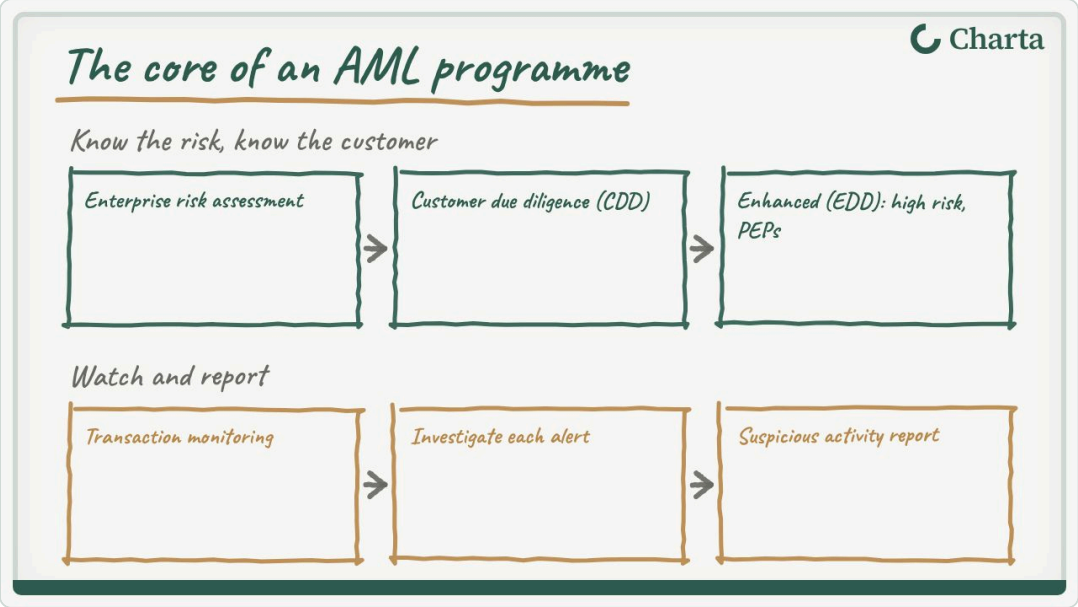
Made-up pattern at a made-up bank

Stage	What Kestrel saw
Placement	Many cash deposits, new accounts
Layering	Fast transfers, abroad and back
Integration	Buys property and a business

IN THE LESSON

- Here is how the three stages looked in Kestrel's own accounts.
- At placement, the customer made many cash deposits into several new business accounts, each a little below the amount that would draw attention.
- At layering, the money was moved quickly between those accounts and sent to accounts in other countries, then partly sent back, with no clear business reason.
- At integration, the funds were used to buy property and a share in a business, so that the money now looked like an ordinary investment.
- Notice where the bank had the best chance.
- The cash deposits and the rapid transfers both passed through Kestrel's own systems, where they could be seen.
- A good A M L programme is built to notice exactly these patterns, which brings us to its parts.

10 The core of an AML programme



IN THE LESSON

- Let us lay out the A M L programme, starting with its core.
- The top row is about knowing the risk and knowing the customer.
- It begins with an enterprise risk assessment, the bank's own view of where laundering could hit it.
- Next comes customer due diligence, or C D D, which means identifying customers and understanding who they are and what they will do with the account.
- For high risk customers, such as politically exposed persons, the bank applies enhanced due diligence, or E D D.
- The bottom row is about watching and reporting.
- Transaction monitoring looks for unusual activity and raises alerts.
- Each alert is investigated by an analyst.
- And where suspicion is confirmed, the bank files a suspicious activity report, or S A R, with the authorities.
- We take each part in turn.

11 The enterprise risk assessment

- Where could laundering hit us, and how badly?
- Score customers, products, countries, channels
- Rate each risk before and after controls
- Sets where staff, systems and rules go
- Refresh it whenever the business changes

IN THE LESSON

- The enterprise risk assessment is the foundation, because everything else is sized from it.
- It asks where laundering could hit the bank, and how badly.
- The bank scores its customers, its products, the countries it deals with, and its delivery channels, such as branches, online accounts or introducers.
- It rates each risk before controls, and again after controls, to see what is left.
- The result tells the bank where its staff, its systems and its monitoring rules should go.
- A private banking desk serving wealthy clients from many countries needs far more attention than a local savings product.
- And the assessment is not a one off exercise.
- It must be refreshed whenever the business changes, which will matter a great deal in the case study.

12 Customer due diligence, standard and enhanced

Know who the customer is, and keep checking

Due diligence step	What it means
Identify and verify	Who is the customer, really?
Owner and purpose	Who controls it; why the account?
Ongoing review	Does activity still fit?
Enhanced, for high risk	Source of funds; senior sign-off
PEPs: a high-risk group	Public role: bribery risk

IN THE LESSON

- Customer due diligence has several steps.
- First, identify the customer and verify that identity against reliable documents.
- Second, understand who owns and controls a company customer, and the purpose of the account.
- Third, keep the review going.
- Due diligence is ongoing, so the bank checks whether the activity still fits what it expected.
- Enhanced due diligence applies to high risk customers.
- It asks for the source of the customer's funds and wealth, and it needs a senior manager to sign off the relationship.
- The best known high risk group is politically exposed persons, or P E Ps.
- These are people who hold or have held a prominent public role, together with their families and close associates.
- They are not criminals, but their position carries a higher risk of bribery and corruption.

13 Example 3: the due diligence workload

200,000 customers. Review high risk yearly, medium every 3 years, low every 5

High risk: 2% = 4,000	4,000 ÷ 1 year	**4,000**
Medium risk: 18% = 36,000	36,000 ÷ 3 years	**12,000**
Low risk: 80% = 160,000	160,000 ÷ 5 years	**32,000**
Reviews a year	4,000 + 12,000 + 32,000	**48,000**
Reviews per working day	48,000 ÷ 240 days	**200**

IN THE LESSON

- Due diligence costs staff time, so let us size it.
- Kestrel has two hundred thousand customers, sorted into three risk tiers.
- High risk customers, including the P E Ps, are two per cent, which is four thousand.
- They are reviewed every year, so four thousand reviews a year.
- Medium risk customers are eighteen per cent, thirty six thousand people, reviewed every three years, which is twelve thousand reviews a year.
- Low risk customers are eighty per cent, one hundred and sixty thousand, reviewed every five years, which is thirty two thousand a year.
- In total, four thousand plus twelve thousand plus thirty two thousand is forty eight thousand reviews a year.
- Over two hundred and forty working days, that is two hundred reviews every working day.
- If the customer base grows, this number grows with it.

14 Transaction monitoring and the alert backlog

Backlog end = Backlog start + New − Cleared
Wait for a new alert ≈ Backlog ÷ cleared a month

Backlog at the end	Alerts waiting for review
Backlog at the start	Last month's closing backlog
New alerts	Raised by the monitoring rules
Alerts cleared	Analysts × alerts each

IN THE LESSON

- Transaction monitoring is a system that applies rules to customers' transactions and raises an alert when something looks unusual, such as a run of cash deposits just below a reporting amount.
- An alert is not a crime.
- It is a question an analyst must answer.
- So a monitoring team works like a queue, and the backlog is the number of alerts waiting for review.
- The backlog at the end of the month equals the backlog at the start, plus the new alerts raised, minus the alerts cleared by analysts.
- If more alerts arrive than are cleared, the backlog grows every month.
- The second line gives a rough guide to delay.
- The wait for a new alert is about the backlog divided by the number of alerts cleared each month.

15 Example 4: Kestrel's growing backlog

12,000 new alerts a month; 40 analysts each clear 250. The backlog starts at zero

New alerts a month	raised by the rules	**12,000**
Cleared a month	40 analysts × 250	**10,000**
Backlog after 6 months	6 × (12,000 − 10,000)	**12,000**
Wait for a new alert	12,000 ÷ 10,000	**1.2 months**
Analysts to keep pace	12,000 ÷ 250	**48**

Clear backlog in 6 months too: (12,000 + 12,000 ÷ 6) ÷ 250 = 14,000 ÷ 250 = 56

IN THE LESSON

- Here are Kestrel's figures.
- Its backlog starts at zero, and its monitoring system raises twelve thousand new alerts a month.
- It has forty analysts, and each clears two hundred and fifty alerts a month, so forty times two hundred and fifty is ten thousand cleared.
- Each month two thousand alerts are left over.
- After six months, six times two thousand is a backlog of twelve thousand alerts.
- A new alert now waits about twelve thousand divided by ten thousand, which is one point two months, before anyone looks at it, a long time for a suspicious payment to sit unread.
- Just to keep pace with new alerts, the bank needs twelve thousand divided by two hundred and fifty, which is forty eight analysts.
- To also clear the backlog of twelve thousand within six months, it must clear another two thousand a month, so fourteen thousand a month, and fourteen thousand divided by two hundred and fifty is fifty six analysts.

16 Monitoring only works if alerts are worked

- An alert is a question, not an answer
- Each one investigated, decided and recorded
- Suspicion confirmed: file a SAR by the deadline
- A backlog means late reports: the money moves on
- Exam: monitoring works only if alerts are worked on time

IN THE LESSON

- This is the second exam point.
- A bank can have excellent monitoring rules and still fail, because an alert on its own protects nothing.
- An alert is a question, not an answer.
- Each one must be investigated, decided and recorded, with the reasons written down.
- Where the analyst confirms a suspicion, the bank must file a suspicious activity report within the deadline the rules set.
- Now see what a backlog does.
- Alerts wait for weeks, the investigations start late, and so the reports go in late or not at all.
- Meanwhile the money has moved on.
- So the exam phrase is that monitoring only works if alerts are investigated and reported on time.
- A system that raises alerts nobody works gives the comfort of control, without the substance.

17 The rest of the AML programme

Five elements that complete the programme

Element	What it does
Sanctions screening	Check names against the lists
Record keeping	Keep evidence of checks
Training	Staff spot and escalate red flags
Named responsible officer	One person accountable
Independent testing	Does it really work?

IN THE LESSON

- The core is not the whole programme.
- Five more elements complete it.
- Sanctions screening checks customers and payments against official sanctions lists, the lists of people, firms and countries the bank must not deal with.
- Record keeping keeps the evidence of identity checks, transactions and investigations, so that the bank can show what it did and why.
- Training teaches staff to spot red flags and escalate them.
- A named responsible officer is one senior person accountable for the A M L programme, so that responsibility cannot drift between departments.
- Last, independent testing checks that the programme really works in practice, not just on paper.
- If Kestrel had tested its monitoring independently, the backlog would have been spotted early.

18 Accountability: three lines of defence

Own it, oversee it, test it

Line	Role in financial crime
1st: the business	Owns risk; runs controls
2nd: compliance	Oversees: policy, rules, challenge
3rd: internal audit	Tests independently

IN THE LESSON

- Who is accountable for all of this?
- The answer follows the three lines of defence.
- The first line is the business.
- The relationship managers and the operations teams own the risk, because they bring in the customers and process the payments, so they run the day to day controls.
- At Kestrel that means the payments team runs the authorisation limits, and the branch runs customer due diligence.
- The second line is compliance.
- It oversees the risk: it writes the policy, sets the monitoring rules, and challenges the business.
- The third line is internal audit, which tests the whole framework independently and reports to the board.
- A common mistake is to say that compliance owns financial crime risk.
- It does not.
- The business owns it.

19 Mistakes to avoid on the framework

Four statements that sound right but are wrong

Mistake	Correction
Segregation stops all fraud	Collusion defeats it
Alerts raised: monitoring works	Only if worked, reported on time
Compliance owns AML risk	Business owns; compliance oversees
Check customers once, at opening	Ongoing; enhanced for high risk

IN THE LESSON

- Before the case study, here are four mistakes to avoid on the framework.
- First, segregation of duties stops all fraud.
- It does not, because collusion defeats it.
- Second, if alerts are being raised, monitoring works.
- It works only if alerts are investigated and reported on time.
- Third, compliance owns A M L risk.
- In fact the business owns it, compliance oversees it, and audit tests it.
- Fourth, a customer is checked once, at opening.
- In fact due diligence is ongoing, and enhanced for high risk customers.
- Hold on to these four, because the case study turns on the second one, and on a bank that let its programme fall behind its own growth.
- That is our next topic.

20 The USAA case: what the case is about

- USAA: a US federal savings bank
- Regulators examined its AML programme
- Central finding: it had not kept pace with the business
- The programme was judged deficient
- Remediation required under an enforcement action

IN THE LESSON

- Now the real case.
- In the case study, U S A A is a U S federal savings bank, that is, a savings bank in the United States supervised at the federal level.
- Its regulators examined its anti money laundering programme.
- Their central finding was that the programme had not kept pace with the business.
- The bank had grown, but its A M L programme had not grown with it.
- Supervisors concluded that the programme was deficient, and they required the bank to fix it under an enforcement action, which is a formal supervisory step that obliges a bank to remediate.
- For the exam, what matters is the pattern of the findings, and the lessons drawn from them.

21 What the regulators found

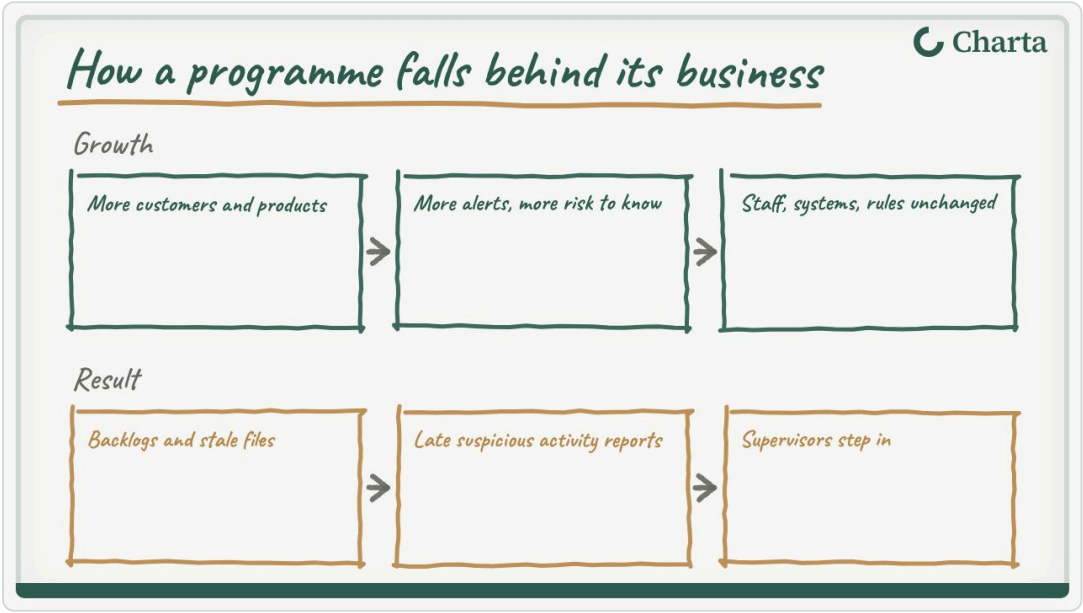
Each finding maps onto a part of the AML framework

Finding	Part of the framework
Weak transaction monitoring	Watch: rules and alerts
Weak customer due diligence	Know the customer
Late SAR investigation and filing	Report
Overall: programme deficient	Remediate under enforcement

IN THE LESSON

- The findings centred on three areas, and each maps onto a part of the framework we just built.
- First, there were weaknesses in transaction monitoring, the watching part of the programme.
- Second, there were weaknesses in customer due diligence, the knowing your customer part.
- Third, there were weaknesses in investigating and filing suspicious activity reports on time, so reports went in late.
- That is the reporting part.
- Put those together and the overall verdict follows: the programme was deficient, and it had to be remediated under enforcement action.
- Notice that the problems were not in one corner.
- They ran through knowing the customer, watching the activity and reporting it, which is most of the core we drew earlier.
- That breadth is the key to the exam point.

22 How a programme falls behind its business



IN THE LESSON

- Why does a programme fall behind?
- Here is the general mechanism behind a finding like this.
- It is a pattern, not extra facts about the case.
- The top row is growth.
- A bank adds customers and products.
- That brings more alerts to investigate and more risk to understand.
- But the staff, the systems and the monitoring rules stay as they were.
- The bottom row is the result.
- Backlogs build, and customer files go stale, because reviews fall behind.
- Suspicious activity reports go in late, because the investigations start late.
- Eventually the supervisors step in.
- Notice that no one in this chain needs to be dishonest.
- Each part of the programme is simply too small for the business it now has to cover.

23 Example 5: budgeting the programme for growth

Made-up figures, not USAA's: Kestrel plans 60% more customers in two years

Customers	200,000 × 1.6	**320,000**
High risk at 2%	2% × 320,000	**6,400**
Alerts a month, in step	12,000 × 1.6	**19,200**
Analysts needed, 250 each	19,200 ÷ 250 = 76.8	**77**
Shortfall against today's 40	77 − 40	**37**

Budget staff, systems and rules into the growth plan

IN THE LESSON

- Let us turn the lesson into a number, using Kestrel again.
- These figures are made up, and they are not U S A A's.
- Kestrel plans sixty per cent more customers in two years, so two hundred thousand times one point six is three hundred and twenty thousand.
- At two per cent, six thousand four hundred will be high risk and need enhanced due diligence.
- If alerts rise in step with customers, twelve thousand times one point six gives nineteen thousand two hundred alerts a month.
- At two hundred and fifty alerts per analyst, that needs seventy six point eight analysts, so seventy seven.
- Kestrel has only forty analysts today, so it is short by seventy seven minus forty, which is thirty seven.
- Staff, systems and rules belong in the growth plan, budgeted before the growth arrives.

24 Lessons from the case, part one

Keep the programme the same size as the business

Lesson	In practice
Scale with growth	Staff, technology, rules grow too
Refresh the risk assessment	New products, customers, markets
Clear the backlogs	Track alert age; add capacity
Meet reporting deadlines	SARs filed on time

IN THE LESSON

- The lessons from the case are general, and they apply to any bank.
- Here is the first group.
- Scale with growth: compliance staffing, technology and monitoring rules must grow with the number of customers and products, as our Kestrel example showed.
- Refresh the risk assessment whenever the business changes, for example when it launches a new product, takes on a new kind of customer, or enters a new market.
- Otherwise the programme is aimed at yesterday's risks.
- Clear the backlogs: track how old the waiting alerts are, and add capacity before the queue gets out of hand.
- And meet the reporting deadlines: suspicious activity reports must be filed on time, every time, because a late report is itself a failure of the programme.

25 Lessons from the case, part two

Accountability at the top, and independent proof that it works

Lesson	In practice
Real board accountability	Gets AML reports and acts
Senior management owns it	Resources match the risk
Independent testing	Test the whole programme

IN THE LESSON

- The second group of lessons is about accountability and assurance.
- First, the board must have real accountability.
- That means it receives meaningful reports on the A M L programme, such as alert backlogs, overdue reviews and late filings, and it acts on them, instead of simply noting them.
- Second, senior management must own the programme, which in practice means making sure its resources match the risk the business takes on.
- A programme that is under staffed is a management decision, even if nobody wrote it down.
- Third, test the programme independently.
- Internal audit, or another independent party, should test the whole programme, end to end, and not just confirm that the policies exist.
- Independent testing is how a bank finds its own backlog before a supervisor does.

26 The exam point: a programme failure

- Not a single rogue employee
- Not a market loss
- A failure of programme design and resourcing
- Fix: rebuild and resource the programme
- Contrast: Kestrel's clerk was one person, local gaps

IN THE LESSON

- Here is the exam point for the case.
- The U S A A failure was not the work of a single rogue employee.
- It was not a market loss either, such as a bad trade or a fall in asset prices.
- It was a failure of programme design and resourcing, spread across the framework: monitoring, due diligence and reporting together.
- That changes what the fix must be.
- Dismissing one person would change nothing, because the programme itself must be rebuilt and properly resourced.
- Compare the fraud at the start of this lesson.
- Kestrel's clerk was one person exploiting gaps in the controls around his own job.
- Both are financial crime risks, but one is an individual breaking the controls, and the other is a programme too small to work.

27 Mistakes to avoid on the case

Wrong answers that examiners like to offer

Wrong answer	Better answer
A rogue employee caused it	Programme design, resourcing
A market or trading loss	An AML compliance failure
Fix: raise more alerts	Work alerts; scale capacity
Compliance alone is to blame	Board, management; business owns

IN THE LESSON

- Here are the wrong answers examiners like to offer about this case, each with a better answer.
- Wrong: a rogue employee caused it.
- Better: it was a failure of programme design and resourcing.
- Wrong: it was a market or trading loss.
- Better: it was an A M L compliance failure, found by supervisors.
- Wrong: the fix is to raise more alerts.
- Better: work the alerts already raised, and scale capacity with the business.
- Wrong: compliance alone is to blame.
- Better: the board and senior management are accountable, and the business owns the risk.
- If an answer choice points to one person, one trade, or one department, be suspicious.
- The case is about a whole programme that did not keep up.

28 Try three quick questions

1. Limit $25,000. Pay $90,000 in equal payments under it. How many?
   Answer: 90,000 ÷ 25,000 = 3.6, so 4 payments of $22,500; a same-payee total catches it.
2. 9,000 alerts a month; 30 analysts clear 280 each. Backlog?
   Answer: Clear 8,400: grows 600 a month. Need 33 analysts.
3. USAA case: what kind of failure?
   Answer: AML programme behind growth: design and resourcing.

IN THE LESSON

- Now try three quick questions.
- Pause the video, think, then listen to the answers.
- Question one.
- A clerk's single signature limit is twenty five thousand dollars, and he wants to pay a fake supplier ninety thousand dollars without a second approver.
- What is the smallest number of equal payments he needs?
- Ninety thousand divided by twenty five thousand is three point six, so four payments of twenty two thousand five hundred dollars.
- A same payee total catches it.
- Question two.
- A team receives nine thousand alerts a month and has thirty analysts who clear two hundred and eighty each.
- What happens?
- They clear eight thousand four hundred, so the backlog grows by six hundred a month, and thirty three analysts are needed to keep pace.
- Question three.
- What kind of failure did regulators find in the U S A A case?
- A deficient A M L programme that had not kept pace with growth, a failure of design and resourcing.