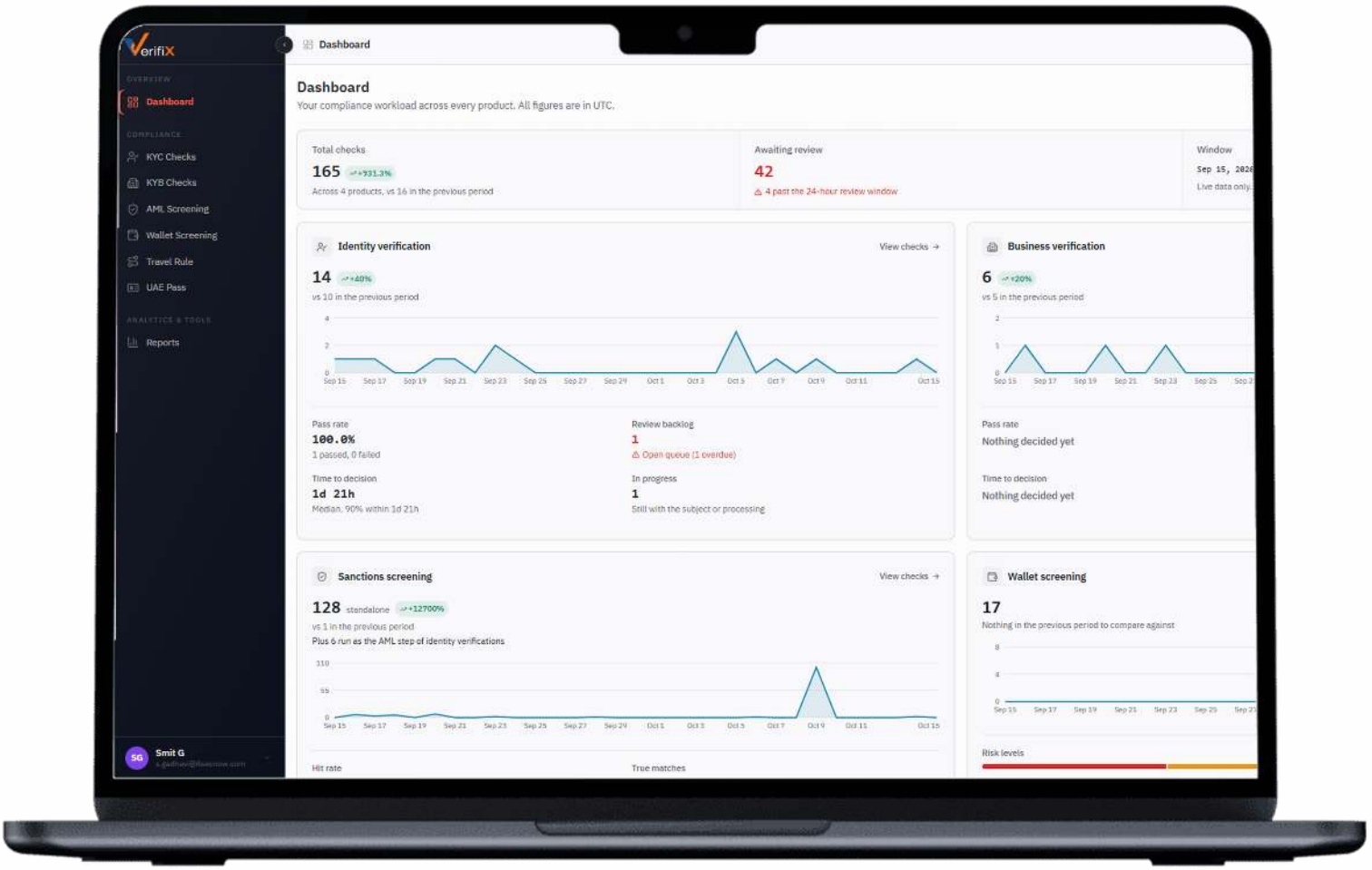
COMPLIANCE INFRASTRUCTURE FOR UAE AND GCC REGULATED ENTITIES

Run compliance in one place — *and defend every decision.*

KYC, KYB, AML screening, blockchain transaction monitoring (KYT) and the Travel Rule in a single decision engine, with case management, versioned risk rules and one audit trail that your compliance team and your engineers can both work from.



REAL VERIFIX DASHBOARD · ILLUSTRATIVE SAMPLE DATA

FIVE CAPABILITY PILLARS, ONE PLATFORM

Run standalone or combined.

01
KYC
Identity verification with document checks and biometric match.

02
KYB
Business and entity verification with UBO discovery.

03
AML
Sanctions, PEP and adverse-media screening with ongoing monitoring.

04
KYT
Blockchain transaction monitoring with wallet risk scoring.

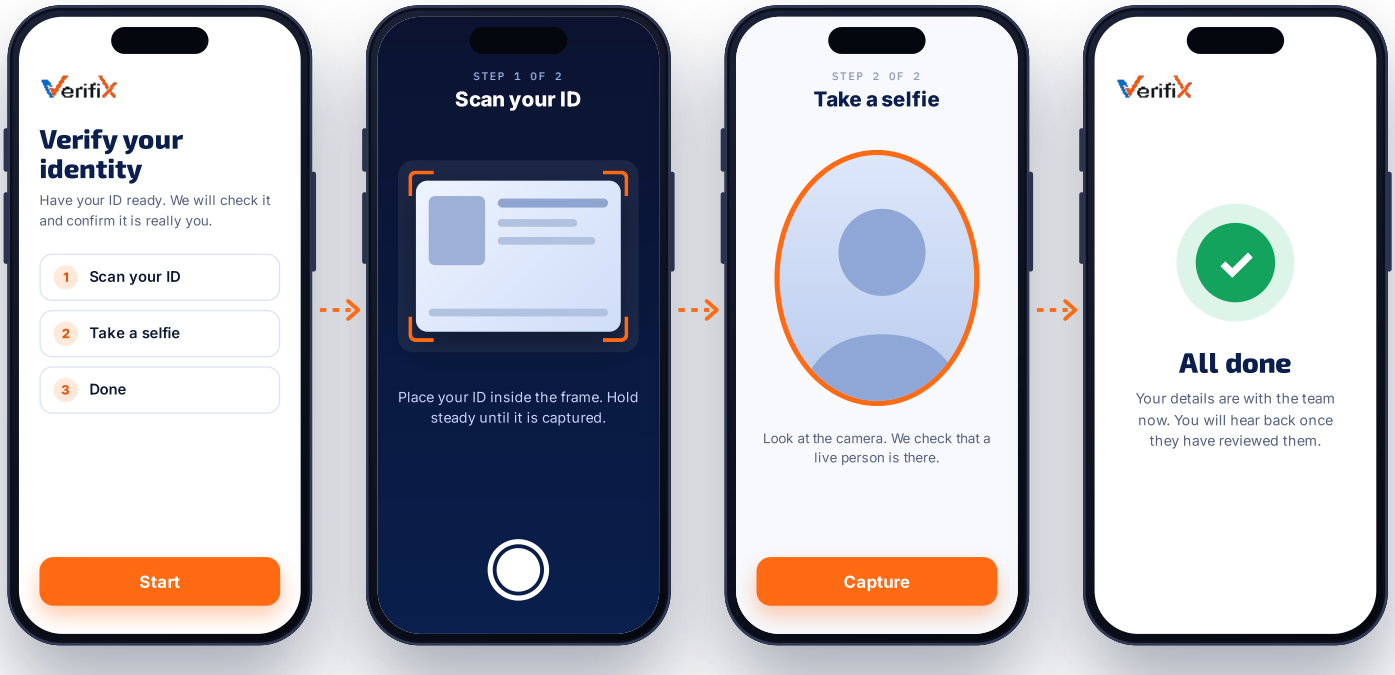
05
Travel Rule
Counterparty VASP data exchange and unhosted-wallet proof of control.

VerifiX

THE CUSTOMER JOURNEY

What your customer does *on their phone*

Your system creates a session and sends the link. Everything after that runs on a hosted page that VerifiX operates, so your team never handles the capture itself.



1 Opens the link

You send the verify link by email or message. Your customer opens it on their phone.

2 Scans their ID

VerifiX confirms the ID is genuine and in date, and reads the details off it.

3 Takes a selfie

Liveness shows a real person is there. Face match shows they are the person on the ID.

4 Waits for your decision

Optional steps such as proof of address or an AML check can be added. Your team makes the final call.

MEANWHILE IN YOUR DASHBOARD

1 Session created — Link sent

• CONFIGURED WORKFLOW
VARA-aligned verification
7 checks · Up to 16 credits

Send verification link

`POST /kyc/sessions → verify_url`

2 Customer verifying — In progress

SK Sara K.

ID · Selfie · Done

Still with the customer on the hosted page.

`Status: in progress`

3 Checks running — In progress

ID document	✓
Liveness	✓
Face match	Running…
AML screening	Queued

`Each check reports on its own`

4 Ready for review — Under review

SK Sara K.

Flagged items wait in the review queue, with a due date.

`kyc.session.in_review`

Hosted page
The customer opens the verify link on their phone

Final say stays with you
Approve, decline, escalate or defer, with a note

Data stays in the UAE
Documents and biometric captures are stored in UAE regions

SIX STEPS · FOUR OWNERS

From customer link to *sealed decision*

Every verification follows the same steps, whether you run one a day or ten thousand. Your team makes the final call on each one.

1 YOUR SYSTEM

Create a session

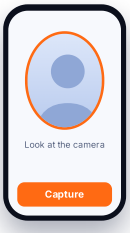
Your server calls the API once per customer and gets a verify link back.

```
POST /kyc/sessions
← response
verify_url: https://…
send to customer
```

2 CUSTOMER

Customer verifies

They scan their ID and take a selfie on the hosted page.



- ✓ Scan the ID
- ✓ Take a selfie
- ✓ Confirm

3 VERIFIX

Checks run

Each check reports its own result as soon as it finishes.

ID document	✓
Liveness	✓
Face match	✓
AML screening	1 hit

4 VERIFIX

Flagged items wait

Anything that needs a person lands in the review queue with a due date.

Sara K.
Review needed
Review window · 24 hours
`kyc.session.in_review`

5 YOUR TEAM

A reviewer decides

Approve, decline, escalate or defer. A note is required.

Approve | Decline
Escalate | Defer
Note (required): reason for the decision

6 VERIFIX

Evidence file is sealed

The case file is kept and can be exported on demand.

Approved
Evidence record sealed
Export case file

WEBHOOK EVENTS ALONG THE WAY

`kyc.session.in_review`	`kyc.session.completed`	`kyc.session.declined`
Checks finished; waits for your team	Approved by your team	Declined by your team

KYC Checks

Identity verification sessions for individuals.

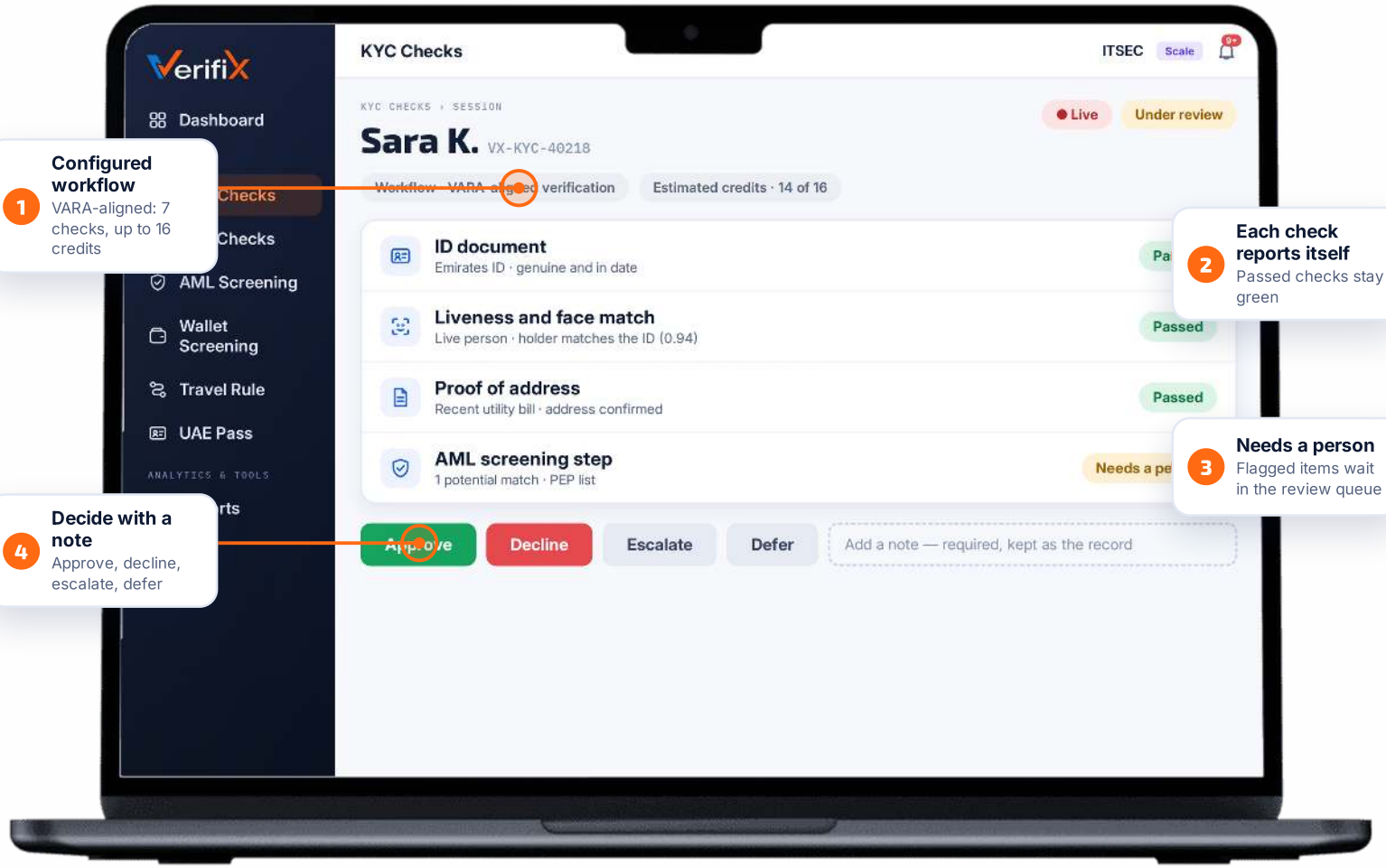
CONFIGURED WORKFLOWS | LIVE AND TEST | REVIEW QUEUE

Who uses it
Compliance analysts and onboarding teams

What you see
One session with every check and its result

Why it matters
Your team makes the final call on every session

Your customer scans their ID and face on a hosted page. VerifiX runs the checks, shows every result on one screen, and your team approves, declines, escalates or defers, with a note that becomes the record.



7
checks in a VARA-aligned workflow

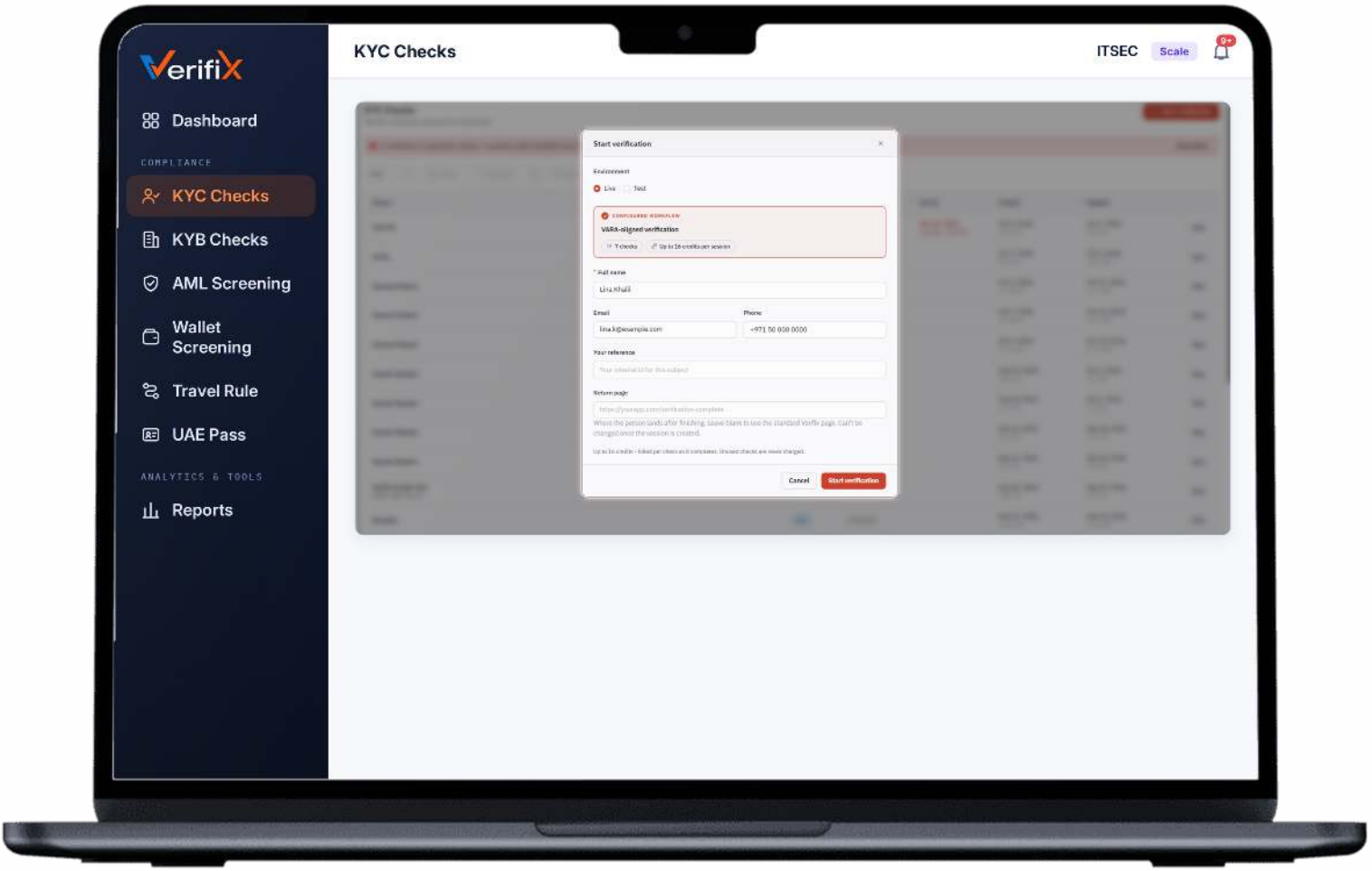
16
credits at most per session

4
ways to decide, with a note

KYC Checks

START VERIFICATION

KYC Checks verifies individuals through a configured workflow. You start a session, the customer completes the checks through a verification link, and your team reviews anything the automated checks could not decide.



HOW IT WORKS

1. Start a verification in Live or Test. The configured workflow shows its checks and maximum credits.
2. The customer completes the checks. Each result appears on the session checklist.
3. A reviewer looks at flagged checks, asks for a resubmission if needed, and records the decision.

WHAT YOU GET

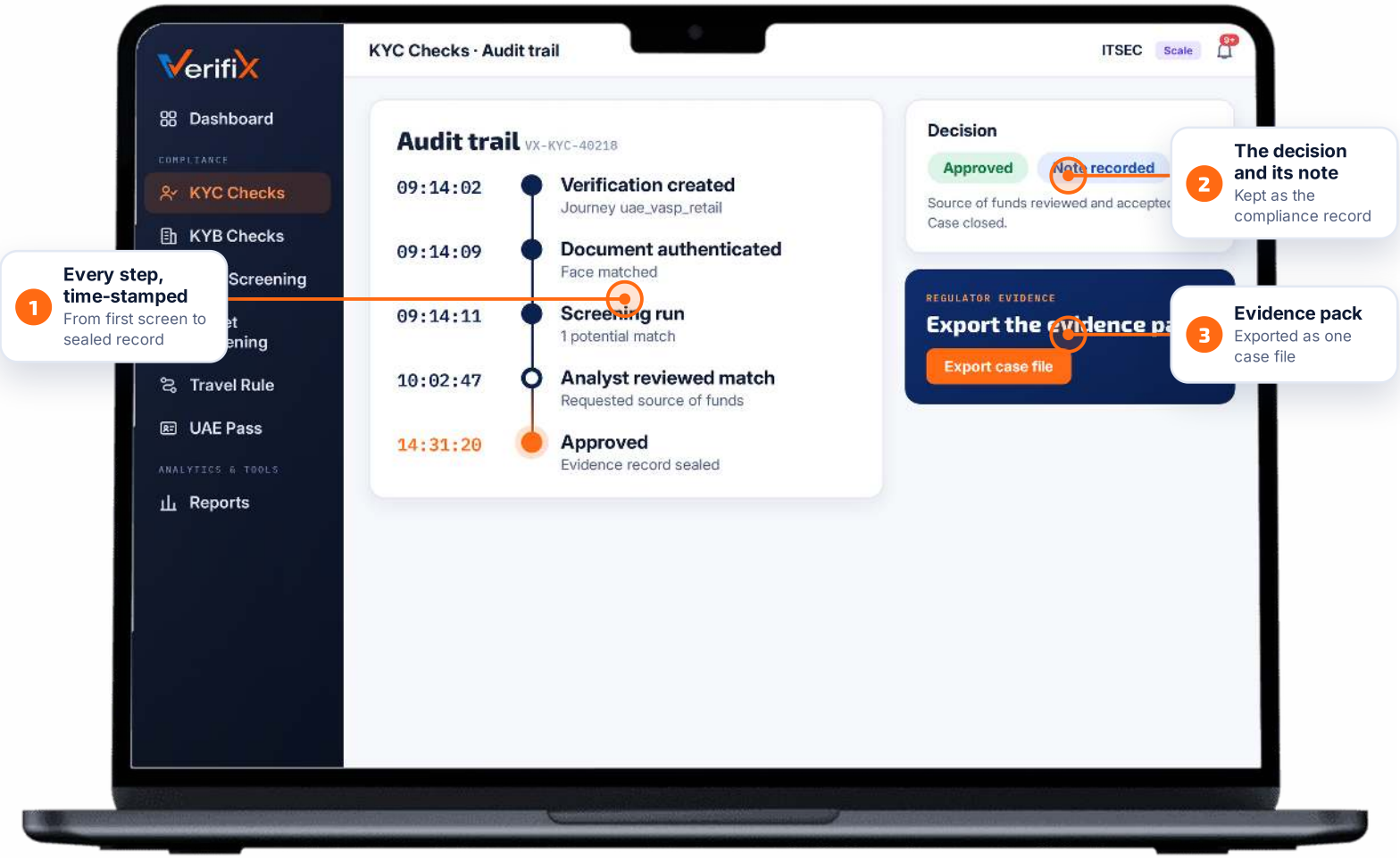
- A configured workflow that shows its checks and maximum credits before you start
- ID document, face match, proof of address, AML screening, due-diligence questionnaire, active liveness and Document AI checks
- A session checklist with stage, resubmissions and review due date
- Results for each check with confidence scores, review, resubmission and a final decision
- A timeline of every provider decision, reviewer action and credit charged
- Live and test environments; test sessions run the same journey

One audit trail, *from first screen to sealed record*

Every step is one row you can export as regulator evidence.

Who uses it	What you see	Why it matters
Reviewers, MLROs and auditors	Every action with time, source and person	Regulator evidence on demand

Documents, screening results, scores and reviewer actions are kept with each decision. Who checked what, when, and on which policy version is recorded automatically, and exported as one case file.



5
steps recorded on this case

1–2,000
characters in the decision note

1
evidence pack sealed per decision

KYB **Checks**

Business verification sessions for companies.

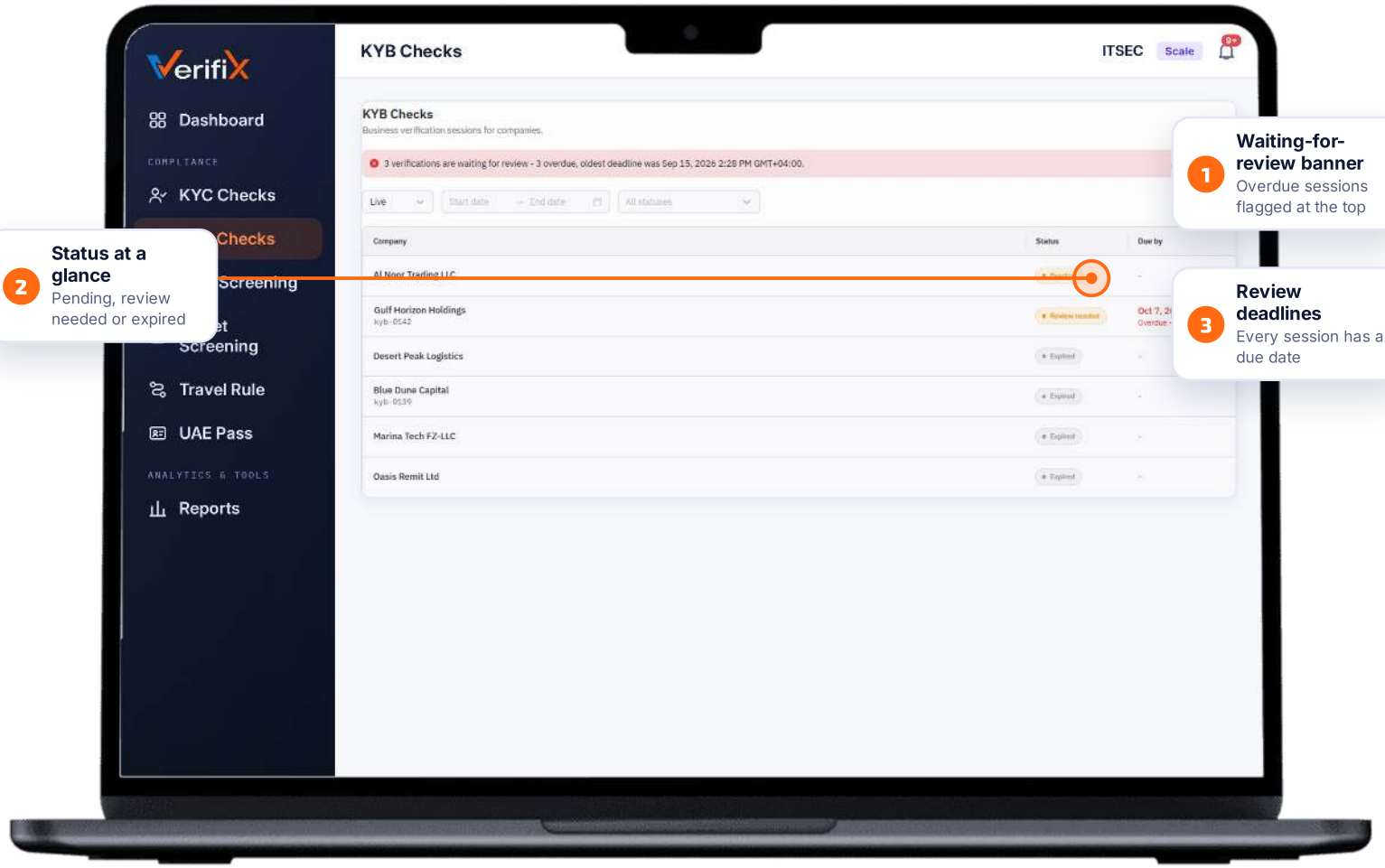
VERIFICATION LINK BY EMAIL | REVIEW DEADLINES

Who uses it
Compliance teams onboarding companies

What you see
Sessions, status and review deadlines

Why it matters
Verify the company and the people behind it

Create a company session with the legal name, country and registration number. Details are prefilled from the register, the company uploads documents, owners and officers are verified, and your team decides.



5
steps from session to decision

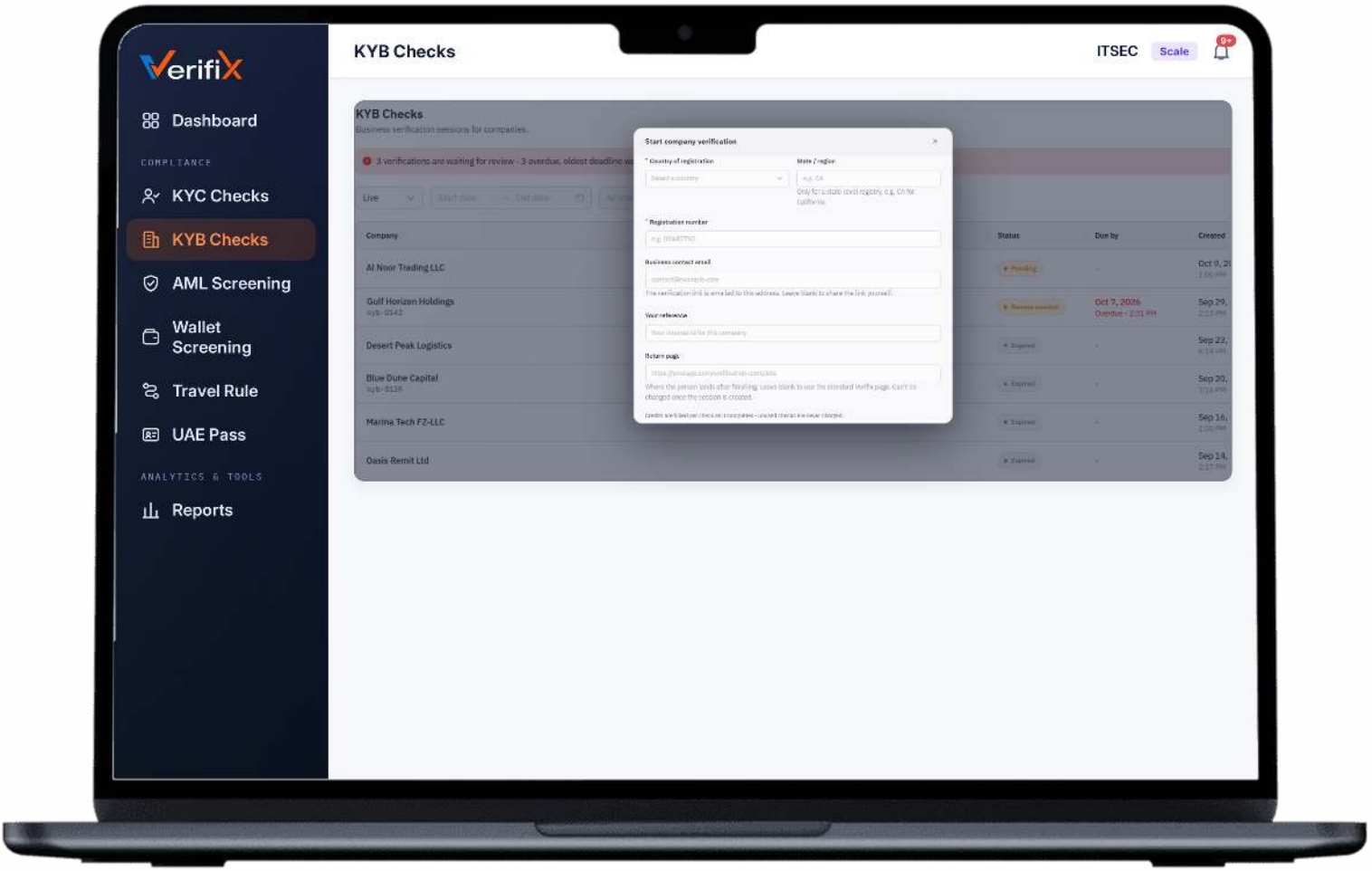
AE
UAE-registered companies

1
verification link by email

KYB Checks

START COMPANY VERIFICATION

KYB Checks verifies companies. You enter the company's registration details, VerifiX sends a verification link to the business contact, and every session is tracked against a review deadline.



HOW IT WORKS

1. Enter the legal name, country of registration and registration number.
2. The verification link goes to the business contact by email, or you share it yourself.
3. Sessions that need a decision wait in the review queue, with overdue items flagged.

WHAT YOU GET

- Company verification by legal name, country of registration and registration number, including state-level registries
- A verification link emailed to the business contact, or shared by you
- A review queue with due dates and overdue alerts
- Status tracking for every session: pending, review needed and expired
- Credits billed per check as it completes; unused checks are never charged

AML Screening

Screen individuals and companies against sanctions, PEP, watchlist, and adverse-media data.

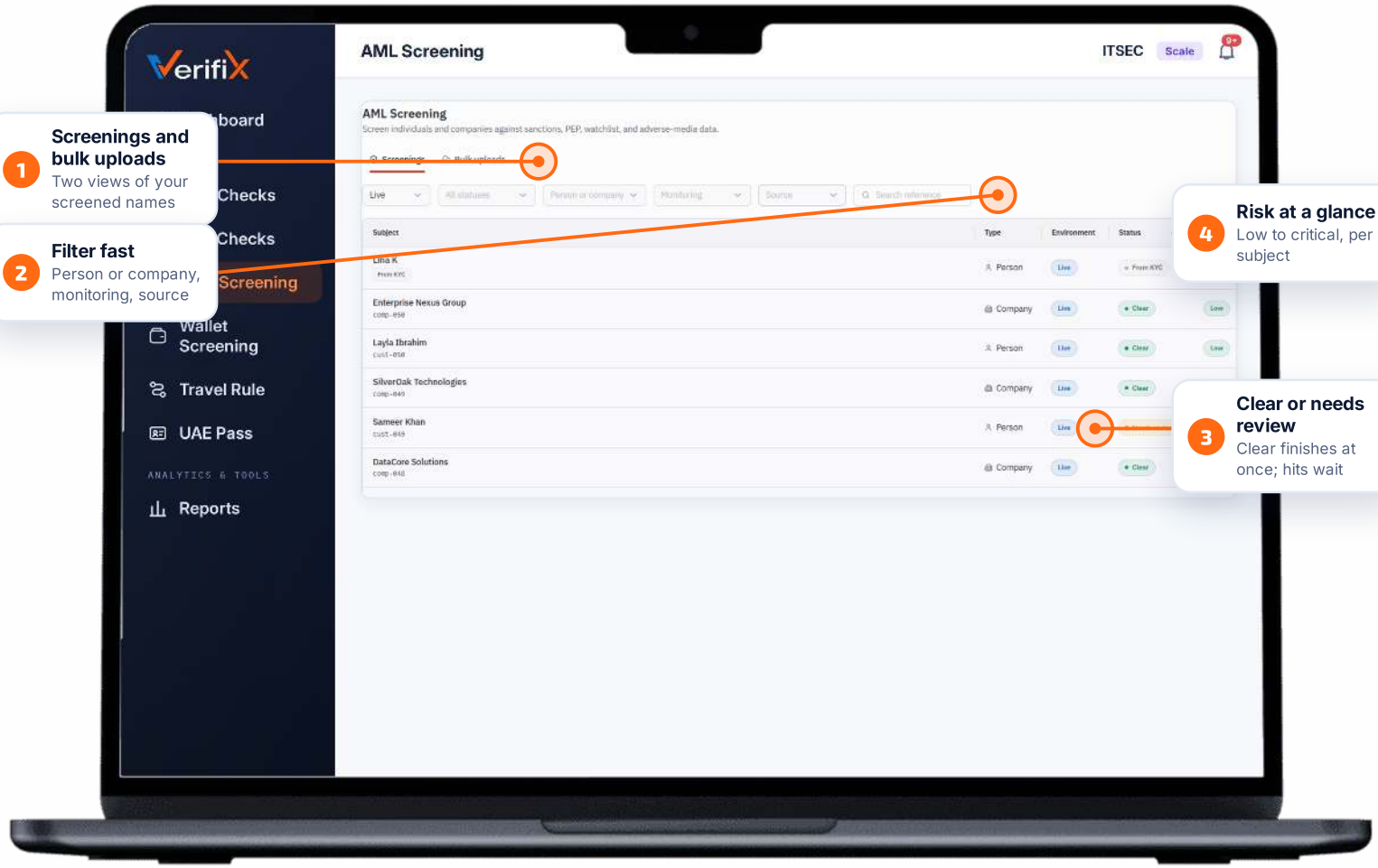
BULK UPLOAD · ONGOING MONITORING · EXTENDED ADVERSE MEDIA

Who uses it
Analysts screening people and companies

What you see
Each subject with status and risk

Why it matters
Screen once, keep watching daily

Check a person or company against sanctions, politically exposed persons and warnings. A clear result finishes at once, any hit waits for review, and ongoing monitoring re-screens daily and reopens a screening only when something new appears.



1,300+
sources searched

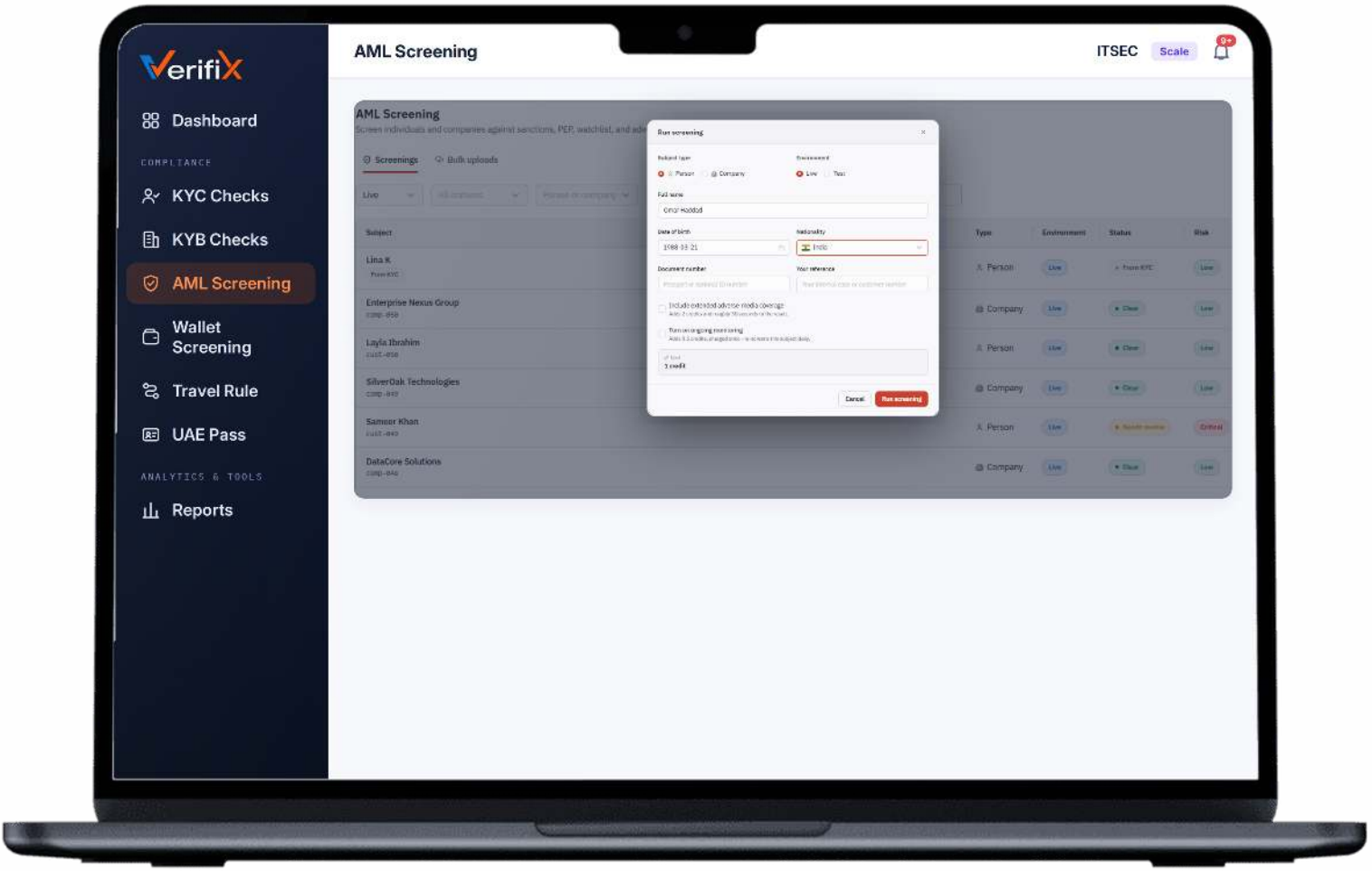
0–100
match score and risk score

Daily
re-screening when monitoring is on

AML Screening

RUN SCREENING

AML Screening checks people and companies against sanctions, PEP, watchlist and adverse-media data. Screen one subject at a time or upload a batch, and keep subjects under ongoing monitoring.



HOW IT WORKS

1. Enter the subject's details, or upload a file of subjects.
2. Add extended adverse-media coverage or daily ongoing monitoring if you need them.
3. Review hits and matches. Each subject shows its status, risk level and timeline.

WHAT YOU GET

- Screening for people and companies, one at a time or by bulk upload
- Optional extended adverse-media coverage
- Optional ongoing monitoring that re-screens the subject daily
- Hits, risk level and status for every subject, with matches to review
- Screenings from KYC sessions mirrored automatically, with the option to promote them to a full screening
- A timeline of every result and action

Wallet **Screening**

Screen crypto wallets and transactions, trace where funds came from, and watch the wallets that matter.

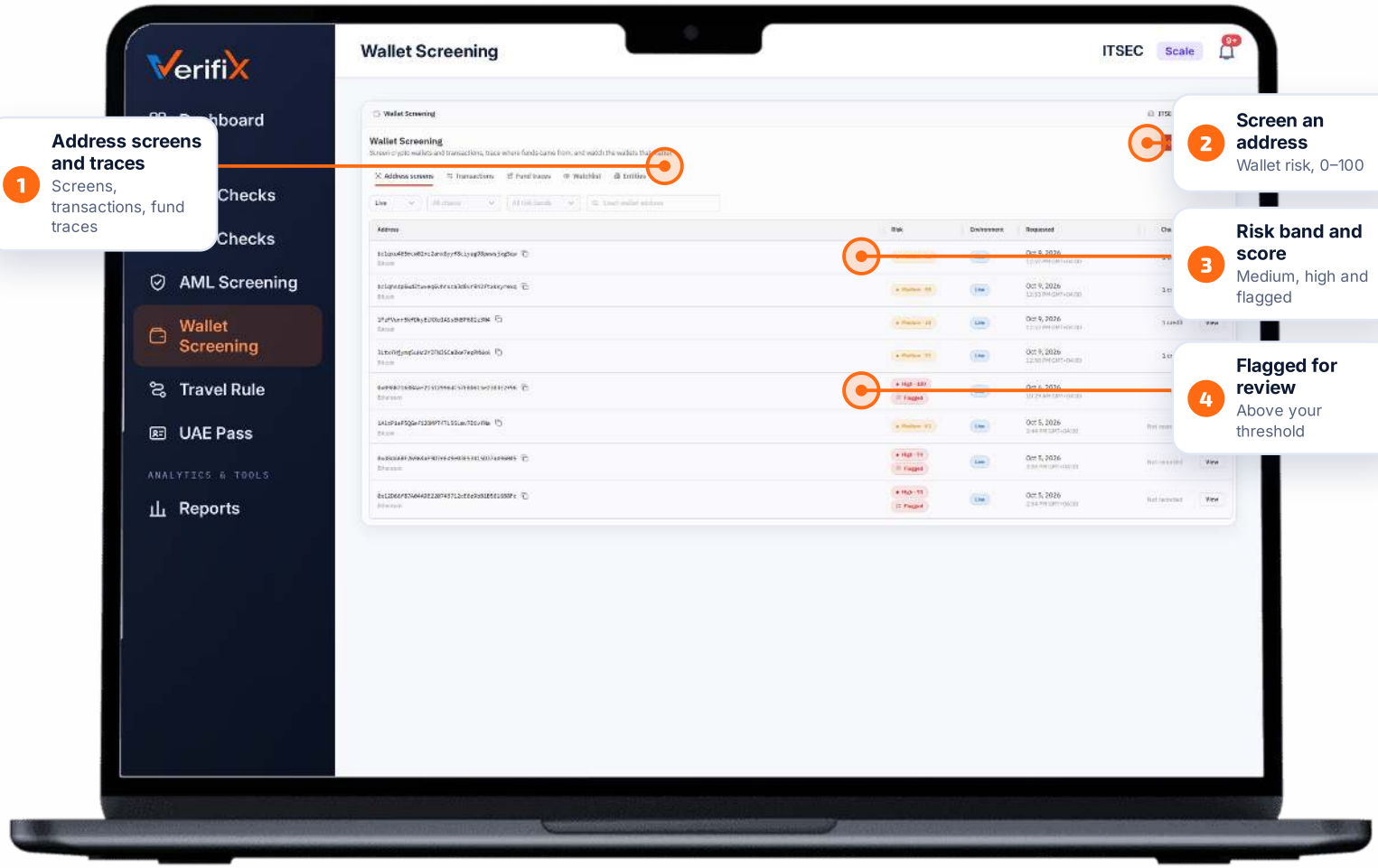
ADDRESS SCREENS · TRANSACTIONS · WATCHLIST · ENTITIES

Who uses it
Crypto compliance and risk teams

What you see
A 0–100 score and band for every address

Why it matters
Know where funds came from before accepting

Screen an address or a transaction, trace funds through hops and amounts, search the entities behind a wallet, or watch an address for changes. Incoming shows where funds came from, outgoing where they went.



Low · 0–29
No meaningful exposure

Medium · 30–69
Worth a look before a large transfer

High · 70–100
Review before accepting funds

0–100
wallet risk score, per address

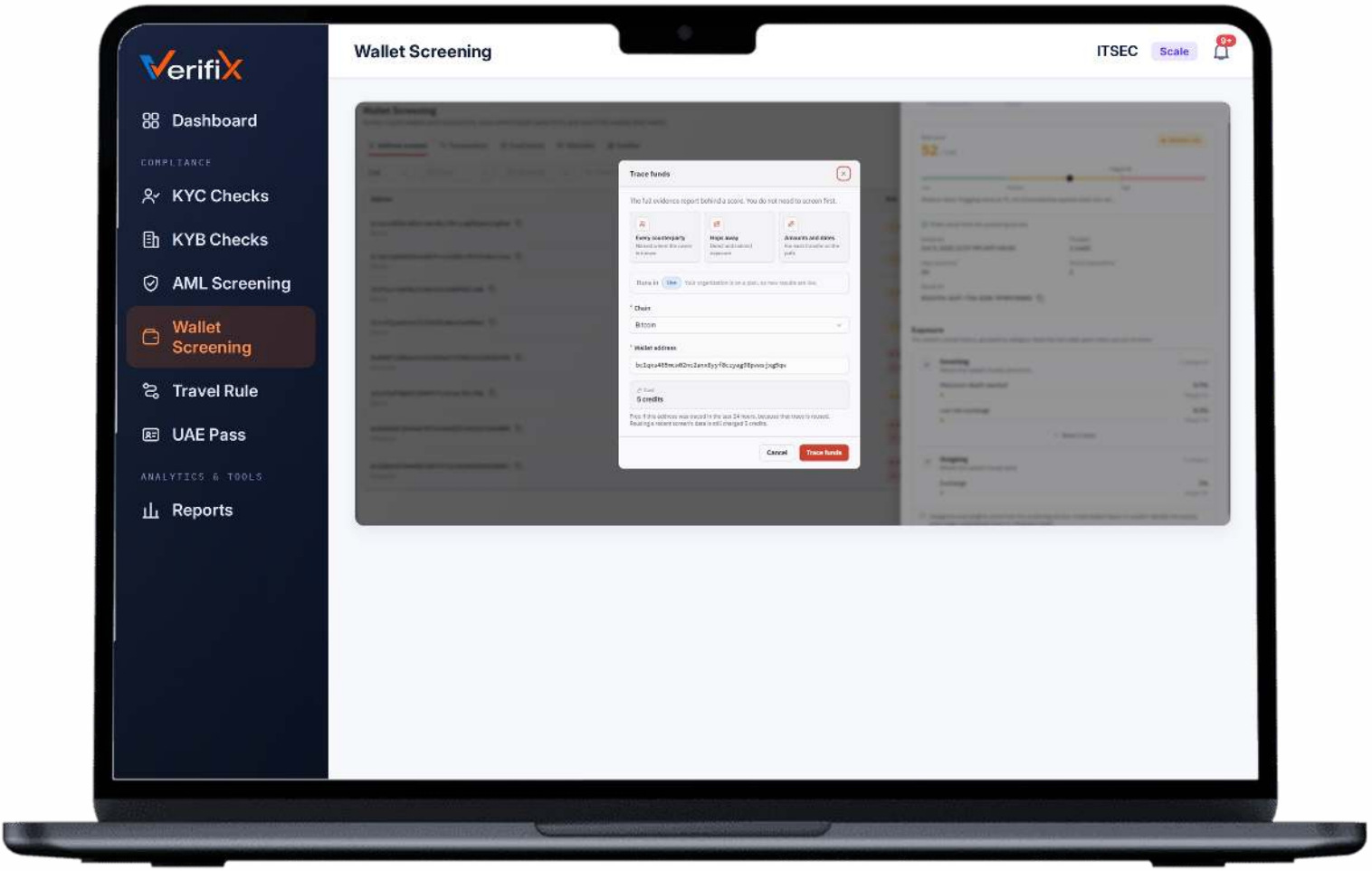
5
actions: screen, trace, search, watch

3
risk bands: low, medium, high

Wallet Screening

TRACE FUNDS

A fund trace is the full evidence report behind a wallet's score. It follows funds across hops to every counterparty, with amounts and dates for each transfer.



HOW IT WORKS

1. Choose the chain and enter the wallet address. You do not need to screen it first.
2. VerifiX traces the funds and lists every counterparty, incoming and outgoing.
3. Review each counterparty's category, distance in hops, share and amount.

WHAT YOU GET

- Every counterparty, named where the owner is known
- Direct and indirect exposure, measured in hops
- Amounts and dates for each transfer on the path
- Incoming and outgoing funds split by counterparty, with share and amount
- Total amount and number of transfers traced
- No charge to reopen an address traced in the last 24 hours

Travel *Rule*

Travel Rule, handled before the transfer leaves.

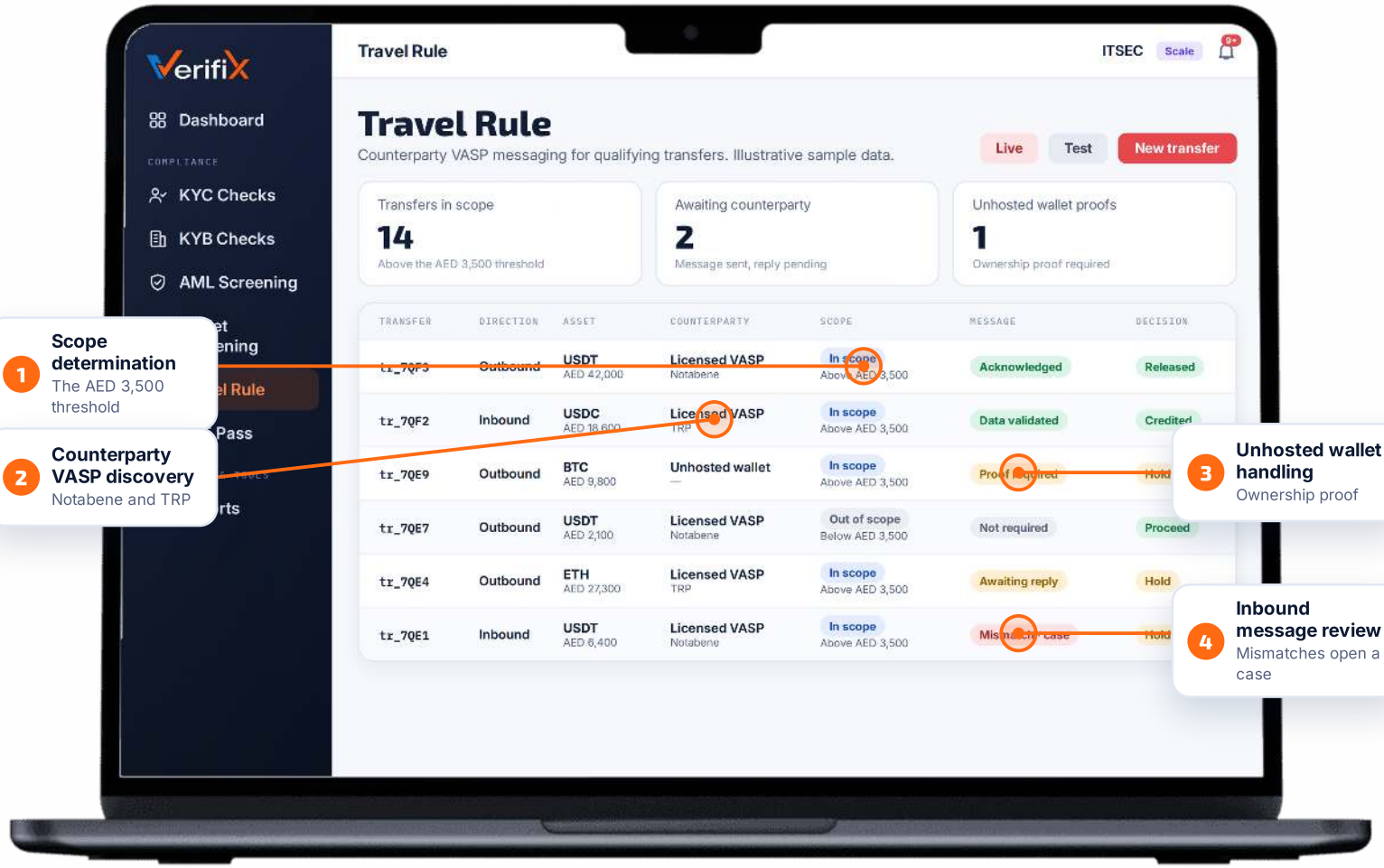
COUNTERPARTY VASP DISCOVERY | NOTABENE AND TRP | UNHOSTED WALLET PROOF

Who uses it
Compliance teams and MLROs at virtual asset firms

What you see
Each transfer with its scope, counterparty, reply and decision

Why it matters
One call covers the Travel Rule and wallet screening

Counterparty VASP discovery, originator and beneficiary data exchange, unhosted-wallet ownership proof, and a message record for every qualifying transfer, evaluated in the same call that screens the wallet.



AED 3,500
Travel Rule threshold in the UAE

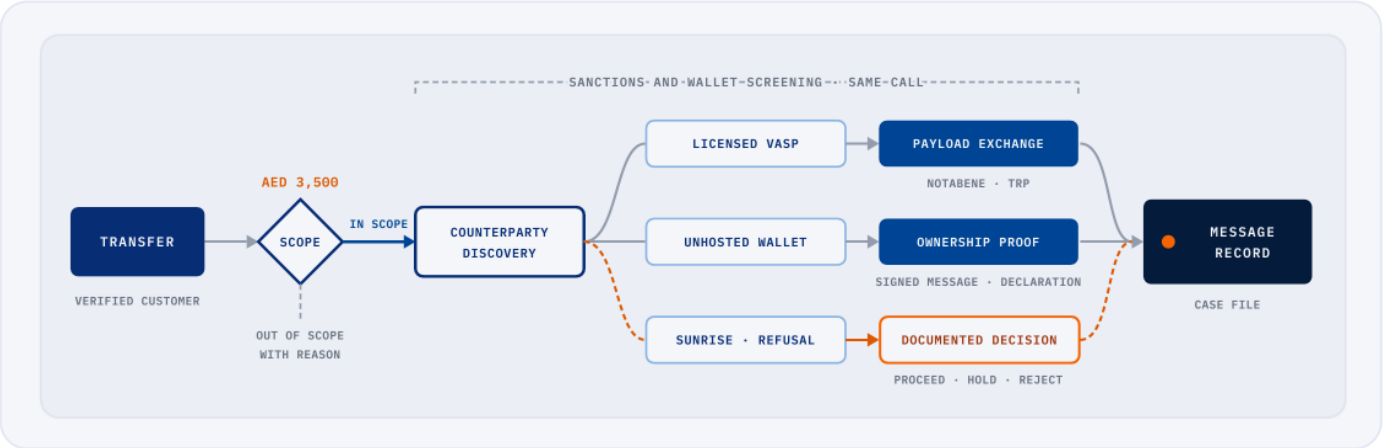
2
messaging protocols: Notabene and TRP

4
Travel Rule modules

Travel *Rule*

Travel Rule, handled before the transfer leaves.

Counterparty VASP discovery, originator and beneficiary data exchange, unhosted-wallet ownership proof, and a message record for every qualifying transfer, evaluated in the same call that screens the wallet.



INSIDE THE HANDSHAKE

What happens before the transfer leaves

Threshold test, counterparty resolution, payload exchange, and the sunrise-case fallback when the other side cannot receive.

01 Scope determination

Every transfer is tested against the applicable threshold and transfer type before any data leaves your tenant, the AED 3,500 threshold.

02 Counterparty VASP discovery

The destination address is attributed to an institution where attribution exists, and matched to a reachable counterparty, counterparties are reached over Notabene and TRP.

03 Originator and beneficiary data

Required originator and beneficiary fields are assembled from the verified customer record rather than re-typed, so the message matches the KYC evidence on file.

04 Unhosted wallet handling

Self-custody destinations trigger ownership proof, declaration, signed message, or in-session verification, self-hosted wallets are evidenced with signed-message or micro-transfer proof.

05 Sunrise and refusal handling

When a counterparty cannot receive a message or refuses to respond, the transfer is routed to a documented decision, proceed, hold, or reject, with the reason recorded.

06 Inbound message review

Incoming originator data is validated against the beneficiary you hold, and mismatches open a case instead of silently crediting the account.

07 Screening in the same call

Sanctions screening of the counterparty parties and wallet exposure scoring run alongside the message, so one decision covers both obligations.

08 Message record

What was sent, what came back, when, and under which protocol version, retained on the customer's case file.

Travel Rule

Submission to settlement

How a transfer clears the rule

The originating side and the beneficiary side of the same exchange, in order.

1. **Submit the transfer**
   Send the transfer against a customer ID that already carries verified identity data, before you broadcast or release funds.
2. **Determine scope and counterparty**
   VerifiX decides whether the transfer is in scope, attributes the destination, and resolves whether it is an institution or an unhosted wallet.
3. **Exchange or prove**
   Originator and beneficiary data is exchanged with the counterparty institution, or ownership proof is collected for a self-custody destination.
4. **Decide and release**
   Hold, proceed, or reject based on the response, the screening result, and your own rules, with the outcome attached to the case.
5. **Retain the evidence**
   The message, the response, the proof, and the decision are written to the append-only audit trail with the operator who approved it.

CHAIN OF CUSTODY

One transfer, as the record shows it

Illustrative sample data for an outbound transfer above the AED 3,500 threshold.

13:07:22	**Transfer submitted** · AED 42,000 equivalent
13:07:22	**In scope** · above AED 3,500 threshold
13:07:23	**Counterparty resolved** · licensed VASP, protocol reachable
13:07:24	**Originator and beneficiary payload sent**
13:07:26	**Counterparty acknowledged** · data accepted
13:07:26	**Message record sealed** · transfer released

POST `/v1/travel-rule/transfers`

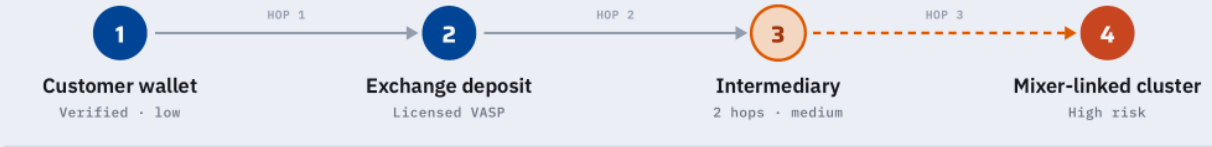
REQUEST

```
curl -X POST https://api.verifix.ae/v1/travel-rule/transfers \
  -H "Authorization: Bearer $VERIFIX_KEY" \
  -d '{
    "direction": "outbound",
    "asset": "USDT",
    "amount": "12500.00",
    "originator": { "customer_id": "cus_2LX..." },
    "beneficiary": { "name": "A. Rahimi", "wallet":
"0x9f2...c41" },
    "jurisdiction": "AE"
  }'
```

RESPONSE

```
{
  "id": "tr_7QF...",
  "in_scope": true,
  "counterparty": {
    "type": "vasp",
    "resolved": "exchange_partner_id",
    "protocol": "supported_protocol",
    "status": "message_sent"
  },
  "beneficiary_response": "pending",
  "hold": true,
  "evidence_id": "ev_31A..."
}
```

TRANSACTION TRACE · 0x9f…c204 — SAMPLE DATA



EXPOSURE	HOPS	ACTION
Indirect	3	Alert raised

Travel Rule

Named modules

The Travel Rule modules

Travel Rule messaging 4 MODULES — Scope the transfer, resolve the counterparty, exchange the payload, and record what was sent, received, or refused.



Travel Rule messaging

`travel_rule`

Exchanges originator and beneficiary information with counterparty institutions on qualifying transfers, and records what was sent, received, or refused.

INPUT	Transfer details and counterparty VASP
RETURNS	message record, counterparty response, unhosted-wallet declaration where applicable



Counterparty VASP discovery

`counterparty_vasp_discovery`

Attributes a destination address to an institution and resolves whether a Travel Rule message can be delivered to it, or whether the destination is an unhosted wallet.

INPUT	Destination address and chain
RETURNS	counterparty type, resolved institution, reachable protocol, sunrise flag



Travel Rule scope test

`travel_rule_scope`

Decides whether a transfer is in scope before any personal data leaves your tenant, using the threshold and transfer rules of the applicable regime.

INPUT	Transfer amount, asset, direction, jurisdiction
RETURNS	in_scope flag with the threshold and rule version applied



Unhosted wallet ownership proof

`unhosted_wallet_proof`

Collects proof that a self-custody destination belongs to your customer: signed message, declaration, or in-session verification, retained as an artefact.

INPUT	Address, customer ID, chosen proof method
RETURNS	proof artefact, method used, verification result

EVIDENCE RETAINED

What proves the payload was exchanged

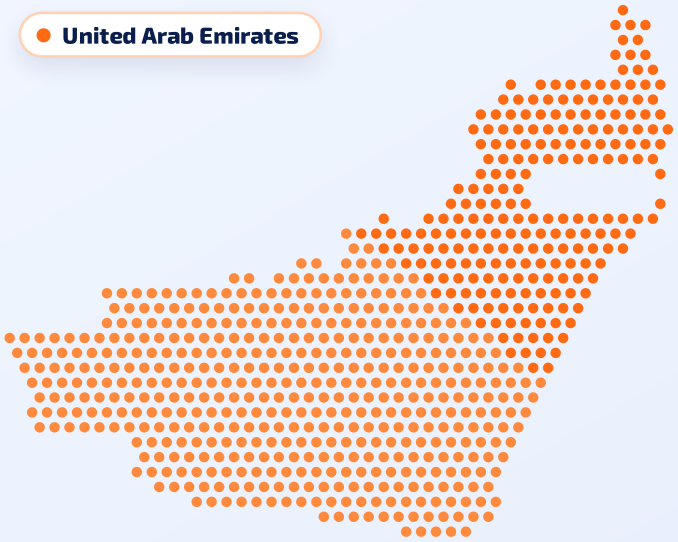
- Scope test applied, with the threshold and rule version used
- Counterparty attribution, institution resolved, and protocol version
- Exact originator and beneficiary fields transmitted, with timestamp
- Counterparty response, refusal, or non-response window
- Unhosted-wallet ownership proof artefact where collected
- Screening results for both parties at the time of transfer
- Final decision, operator identity, and reason code

SCOPE	`in_scope` `out_of_scope` with reason
COUNTERPARTY	`vasp` `unhosted` `unattributed`
DECISION	`proceed` `hold` `reject`
DELIVERY	API response + webhook on counterparty reply
RETENTION	Set to the period your license requires

UAE DATA RESIDENCY · DEFAULT, NOT AN ADD-ON

Hosted in the UAE. Designed for UAE data law.

Compliance data is the most sensitive data you hold. On VerifiX, identity documents, biometric captures, screening results, case files and the audit trail are stored in UAE regions on AWS and Microsoft Azure: in-country by default, not as a paid add-on.



STORED IN UAE REGIONS · AWS / AZURE

- Identity documents
- Biometric captures
- Screening results
- Case files
- Audit trail
- Databases and keys

Run by a UAE cybersecurity company

Built, operated and security-tested by ITSEC, Dubai, est. 2011.

ISO/IEC 27001 · ISO 22301

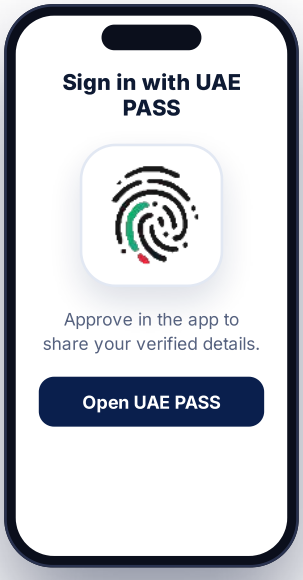
Designed for UAE data protection law

UAE PDPL (Federal Decree-Law No. 45 of 2021), plus DIFC and ADGM rules.

UAE PDPL · DIFC · ADGM

Transparent by contract

Residency scope and named sub-processors are confirmed in your contract.



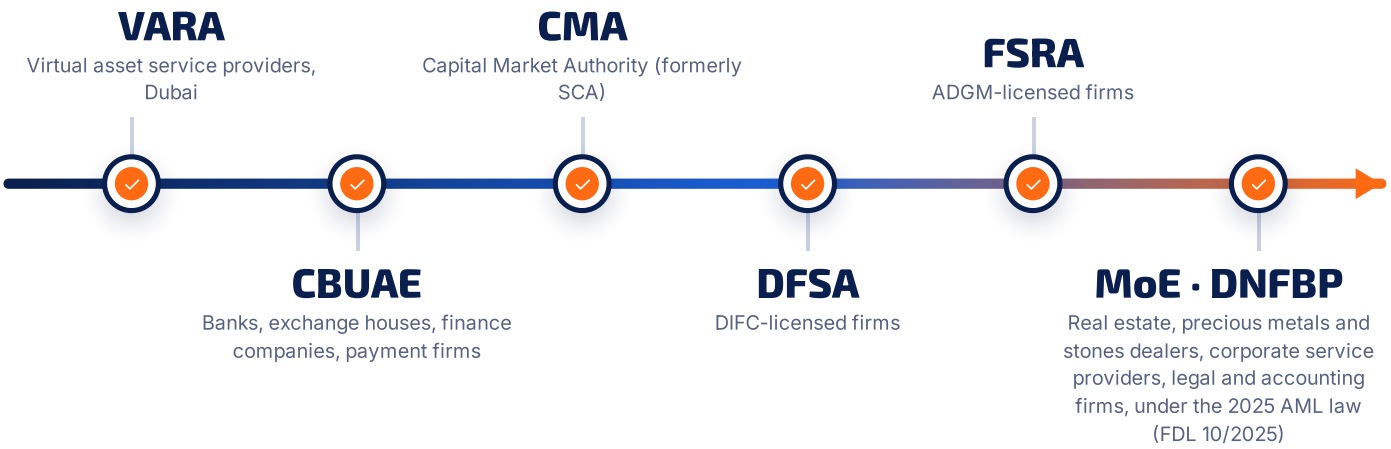
UAE PASS onboarding, inside the same journey

Residents verify with the national digital ID: one tap instead of a document scan. It becomes one more method inside the same session, case record and audit trail. Customers without a full account fall back to a document check.

1. Customer taps UAE PASS
2. Approves in the app
3. Verified details arrive
4. Liveness + face match (optional)
5. Your team decides

YOUR REGULATOR'S JOURNEY, ALREADY BUILT

UAE regulator journeys, pre-configured



- Start from the journey for your licence
- Tune thresholds to your risk appetite
- No blank rule builder

ALSO CONFIGURED ON REQUEST: KSA · Qatar · Bahrain · Kuwait · Oman

Journey templates are a starting point, not legal advice. Regulator names describe the frameworks VerifiX supports and do not imply endorsement, approval or affiliation.

GETTING STARTED

Sandbox on day one — then your first live decision.

SANDBOX · FREE CREDITS · YOU VERIFY YOURSELF

STEP 1 — Sign up
With your work email.

STEP 2 — Create your organization
You become its owner.

STEP 3 — Claim 100 sandbox credits
About eight sandbox verifications.

STEP 4 — Create a sandbox key
Prefix vfx_sandbox_, shown once.

STEP 5 — Verify yourself
Same checks and prices as live.

GO LIVE · YOUR CUSTOMERS · PLAN CREDITS

STEP 6 — Subscribe, pick the workflow
Owner selects the VARA-aligned journey.

STEP 7 — Create a live key
Prefix vfx_live_ with IP allowlist.

STEP 8 — First live session
Watch the signed webhook arrive.

GOOD TO KNOW

Sandbox credits are forfeited when you subscribe, so finish your testing first. A key works in one environment only.

`vfx_sandbox_••••` `vfx_live_••••`

PLATFORM DETAILS

Platform at a glance

INTEGRATION	One REST API and signed webhooks across all five pillars; SDKs and a hosted flow. Sandbox and production keys issued together.
IDENTITY AND SSO	SAML 2.0, OIDC and SCIM. Four-eyes review on cases.
MODULES	**39** individually switchable, separately auditable checks across identity, documents, biometrics, fraud signals, business structure, screening and chain analytics.
COVERAGE	Country, document and sanctions-list coverage shared on request · Arabic and English
TRAVEL RULE	Originator and beneficiary data exchange with counterparty VASPs over Notabene and TRP, with unhosted-wallet proof of control. Thresholds configured to your regulator's requirement.
REPORTING	goAML / STR export support.
GO-LIVE	Sandbox on day one.
COMMERCIALS	Per check and per volume, quoted in AED or USD; modules you switch off are not billed. Starter plans for smaller firms. Retention and availability set in your contract.



WHO IT IS FOR

Built for regulated sectors

- **VASPs**
- **Banking**
- **Capital markets**
- **Fintech, payments and remittance**
- **Exchange houses**
- **Insurance and takaful**
- **DNFBPs: real estate, precious metals and stones, corporate service providers, legal and accounting**

NEXT STEP

See VerifiX against your own onboarding flow.

Tell us your licence and we will show you the journey already built for it.

Book a demo | Request a sandbox

SCAN TO BOOK A DEMO

TALK TO US +971 55 638 9560 sales@verifix.ae

Screens use illustrative sample data. VerifiX is a product of ITSEC LLC FZ, Dubai — est. 2011 · Version 2.0 · October 2026.