Runbook: Sumsub KYC Failure

Runbook: Sumsub KYC/AML Verification Failure

Service: Sumsub Identity Verification (KYC/AML) **Severity:** HIGH (blocks new user registrations) **MTTR Target:** <30 minutes **Owner:** John (AI Director)

Overview

Sumsub provides automated identity verification (KYC - Know Your Customer) and AML (Anti-Money Laundering) checks for Drop. Required for regulatory compliance before users can make payments.

KYC Process:

1. User uploads ID document (passport, driver's license, national ID)
2. User takes selfie (liveness check)
3. Sumsub verifies document authenticity
4. Sumsub performs AML sanctions screening
5. Result: APPROVED, REJECTED, or MANUAL_REVIEW

Impact: If Sumsub fails, new users cannot complete registration. Existing users are unaffected.

Symptoms

Users report they cannot complete identity verification:

- ID upload fails with error
- Verification stuck at "Processing..." indefinitely
- Error message: "Verification service unavailable"
- Webhook never receives result from Sumsub
- User status stuck at "pending_kyc"

User impact: Cannot complete registration, cannot make payments.

Diagnosis

1. Check Sumsub Service Status

External status:

```
# Sumsub does not have a public status page
# Test via API health check
curl https://api.sumsub.com/resources/healthcheck \
  -H "X-App-Token: <app-token>" \
  -v

# Expected: HTTP 200
# If 500/503: Sumsub outage
```

2. Check Drop Logs

```
# CloudWatch Logs (production)
aws logs filter-log-events \
  --log-group-name /aws/apprunner/drop-production \
  --filter-pattern "sumsub" \
  --start-time $(date -u -d '30 minutes ago' +%s)000 \
  --region eu-west-1

# Look for:
# - "Sumsub API timeout"
# - "Sumsub webhook failed"
# - "KYC verification failed: document_expired"
# - "AML sanctions match: [name]"
```

3. Check Sumsub Dashboard

```
# Login to Sumsub Dashboard
open https://cockpit.sumsub.com

# Check:
```

```
# - Recent applicants (last 1 hour)
# - Failed verifications
# - Manual review queue length
# - Webhook delivery status
```

4. Check Webhook Delivery

Verify webhook endpoint is reachable:

```
# Sumsub sends webhooks to: https://getdrop.no/api/webhooks/sumsub
# Test endpoint manually
curl -X POST https://getdrop.no/api/webhooks/sumsub \
  -H "Content-Type: application/json" \
  -H "X-Sumsub-Signature: test" \
  -d '{"type":"applicantReviewed","reviewResult":{"reviewAnswer":"GREEN"}}' \
  -v

# Expected: HTTP 200
# If 404: Webhook endpoint not deployed
# If 401: Signature validation issue
```

5. Test KYC Flow

Manual test (staging):

```
# 1. Create test applicant
curl -X POST https://api.sumsub.com/resources/applicants \
  -H "X-App-Token: <sandbox-app-token>" \
  -H "Content-Type: application/json" \
  -d '{
    "externalUserId": "test-user-123",
    "levelName": "basic-kyc-level",
    "email": "test@example.com"
  }' \
  -v

# Expected: HTTP 201, applicant created
# If 400: Invalid request
# If 500: Sumsub API issue
```

Common Causes & Solutions

Cause 1: Sumsub API Outage (External)

Probability: 5% (Sumsub service disruption)

Symptoms:

- All KYC verifications fail
- Sumsub API health check returns 503
- Dashboard shows no recent applicants
- Logs show API timeouts

Solution:

1. **Verify outage:**

```
# Test Sumsub API from different networks
curl https://api.sumsub.com/resources/healthcheck \
  -H "X-App-Token: <app-token>" \
  -v

# If consistent failure: confirmed outage
```

2. **Contact Sumsub support:**
   - Email: support@sumsub.com
   - Live chat: https://cockpit.sumsub.com (bottom-right)
   - Phone: Check Sumsub Dashboard for support number
3. **Communicate to users (Norwegian):**

```
Emne: Identitetsverifisering midlertidig utilgjengelig

Hei,

Vi opplever for øyeblikket tekniske problemer med identitetsverifisering.
Du kan fortsette registreringen senere.

Vi forventer at tjenesten er tilbake innen [X minutter/timer].

Mvh,
```

```
Drop
```

4. **Queue pending verifications:**

```
-- Mark users as pending KYC retry
UPDATE users
SET kyc_status = 'pending_retry',
    kyc_retry_at = datetime('now', '+1 hour')
WHERE kyc_status = 'pending_kyc'
AND created_at > datetime('now', '-2 hours');
```

5. **Retry when Sumsub is back:**

```
# Cron job to retry pending KYC
node ~/ALAI/products/Drop/scripts/retry-kyc.js
```

ETA: Depends on Sumsub (typically <2 hours)

Cause 2: Document Verification Failure (User Error)

Probability: 40% (user uploads poor quality or invalid document)

Symptoms:

- Specific users fail KYC (not all users)
- Logs show: "document_not_readable", "document_expired", "document_type_mismatch"
- Sumsub dashboard shows rejection reason

Common rejection reasons:

- Blurry photo (document not readable)
- Expired document (passport/ID expired)
- Wrong document type (e.g., bank statement instead of ID)
- Photo cropped (missing corners/edges)
- Underage (user < 18 years old)

Solution:

1. **Identify rejection reason:**

```
SELECT user_id, kyc_rejection_reason, kyc_rejected_at
FROM users
WHERE kyc_status = 'rejected'
ORDER BY kyc_rejected_at DESC
LIMIT 10;
```

2. **Show clear error to user (Norwegian):**
   Blurry document:

```
Dokumentet er ikke leselig
Ta et nytt bilde i godt lys.
Sørg for at all tekst er skarp og leselig.
```

   Expired document:

```
Dokumentet er utløpt
Vennligst last opp et gyldig pass eller førerkort.
Dokumentet må være gyldig i minst 1 måned.
```

   Wrong document type:

```
Feil dokumenttype
Vi godtar kun: Pass, Nasjonalt ID-kort, Førerkort.
Bankkort og regninger godtas ikke.
```

   Underage:

```
Du må være 18 år eller eldre
Drop er kun tilgjengelig for brukere over 18 år.
```

3. **Allow user to retry:**
   - Show "Try Again" button in app
   - Provide tips for better photo quality
   - Link to FAQ: "How to take a good ID photo"
4. **Track retry success rate:**

```
-- How many users succeed on 2nd attempt?
SELECT
  COUNT(*) FILTER (WHERE kyc_attempt = 1 AND kyc_status = 'approved') as
first_attempt_success,
  COUNT(*) FILTER (WHERE kyc_attempt = 2 AND kyc_status = 'approved') as
second_attempt_success,
  COUNT(*) FILTER (WHERE kyc_attempt >= 3) as multiple_retries
FROM users;
```

ETA: Immediate (user must retry with better document)

Cause 3: AML Sanctions Match (Compliance Issue)

Probability: 3% (user flagged by sanctions screening)

Symptoms:

- Specific user's KYC fails with: "AML_SANCTIONS_MATCH"
- Sumsub dashboard shows "Red flag" or "Manual review required"
- User name matches sanctions list (OFAC, EU, UN, etc.)

Solution:

1. **Identify flagged users:**

```
SELECT user_id, email, full_name, kyc_rejection_reason
FROM users
WHERE kyc_rejection_reason LIKE '%sanctions%'
OR kyc_status = 'manual_review_aml';
```

2. **Review Sumsub dashboard:**
   - Login: https://cockpit.sumsub.com
   - Navigate to applicant
   - Check AML screening results
   - Review sanctions list match details
3. **False positive (common names):**
   - Example: "Ali Hassan" may match many sanctioned individuals
   - Sumsub shows match details (date of birth, nationality)
   - If clearly different person: manually approve in Sumsub
4. **True positive (actual sanctions match):**
   - **DO NOT approve.** This is a legal/regulatory issue.
   - Reject user registration immediately
   - Document incident for compliance records
5. **Notify user (if false positive, manually approved):**

```
Din identitetsverifisering er godkjent
Takk for tålmodigheten. Du kan nå bruke Drop.
```

6. **Notify user (if true positive, rejected):**

```
Vi kan dessverre ikke godkjenne din registrering
På grunn av regulatoriske krav kan vi ikke tilby tjenester til deg.
Ta kontakt med support@getdrop.no hvis du mener dette er en feil.
```

7. **Escalate to Alem if uncertain:**
   - AML compliance is critical
   - False rejection = bad UX, but false approval = legal risk
   - Alem makes final call on borderline cases

ETA: 10 minutes (false positive), N/A (true positive - reject)

Cause 4: Webhook Delivery Failure

Probability: 15% (Drop webhook endpoint down or unreachable)

Symptoms:

- Sumsub completes verification, but Drop never updates user status
- Logs show: "Webhook not received"
- Sumsub dashboard shows "Webhook delivery failed"
- User stuck at "pending_kyc" despite Sumsub showing "approved"

Solution:

1. **Check webhook endpoint health:**

```
# Test webhook endpoint
curl -X POST https://getdrop.no/api/webhooks/sumsub \
  -H "Content-Type: application/json" \
  -d '{"type":"ping"}' \
  -v

# Expected: HTTP 200
# If 404/500: Drop webhook endpoint broken
```

2. **Check Sumsub webhook delivery logs:**
   - Login: https://cockpit.sumsub.com
   - Navigate to Settings → Webhooks
   - Check recent delivery attempts
   - Look for: 404, 500, timeout errors
3. **Manually retry failed webhooks:**
   - Sumsub Dashboard → Applicant → "Resend Webhook"
   - This triggers new webhook delivery to Drop

- Verify Drop receives and processes it

4. **Fetch verification results via API (if webhook lost):**

```
# Manually fetch applicant status from Sumsub
curl -X GET https://api.sumsub.com/resources/applicants/<applicant-id>/status \
  -H "X-App-Token: <app-token>" \
  -v

# Parse result and update Drop database
```

5. **Update Drop database manually:**

```
UPDATE users
SET kyc_status = 'approved',
    kyc_approved_at = datetime('now')
WHERE sumsub_applicant_id = '<applicant-id>';
```

6. **Fix webhook endpoint (if broken):**
   - Check App Runner deployment status
   - Verify webhook route exists: `src/app/api/webhooks/sumsub/route.ts`
   - Check signature validation (Sumsub signs webhooks with HMAC)

ETA: 10 minutes (manual retry), 30 minutes (if endpoint fix needed)

Cause 5: Invalid or Expired API Credentials

Probability: 5% (after credential rotation)

Symptoms:

- Logs show: "401 Unauthorized" or "403 Forbidden"
- All Sumsub API calls fail
- Webhook signature validation fails

Solution:

1. **Verify Sumsub API credentials:**

```
bw get item "Sumsub API" --session $BW_SESSION

# Check:
# - App Token is correct
# - Secret Key is correct (for webhook signature)
```

```
# - Environment: production vs sandbox
```

2. **Regenerate API credentials (if needed):**
   - Login: https://cockpit.sumsub.com
   - Navigate to Settings → API
   - Generate new App Token + Secret Key
   - Copy to Vaultwarden
3. **Update App Runner environment variables:**

```
aws apprunner update-service --service-arn <ARN> \
  --instance-configuration "EnvironmentVariables={
    SUMSUB_APP_TOKEN=<new-app-token>,
    SUMSUB_SECRET_KEY=<new-secret-key>,
    SUMSUB_ENVIRONMENT=production
  }"
```

4. **Trigger deployment:**

```
aws apprunner start-deployment --service-arn <ARN> --region eu-west-1
```

5. **Test after deployment:**

```
# Try creating test applicant
curl -X POST https://getdrop.no/api/kyc/initiate \
  -H "Authorization: Bearer <test-user-token>" \
  -v

# Expected: HTTP 200, Sumsub applicant created
```

ETA: 10 minutes

Cause 6: Liveness Check Failure (Selfie)

Probability: 20% (user fails selfie/liveness verification)

Symptoms:

- Specific users fail at selfie stage
- Logs show: "liveness_check_failed", "face_mismatch"
- Sumsub dashboard shows "Selfie does not match ID photo"

Common reasons:

- Poor lighting (too dark, too bright)
- User wears sunglasses/hat
- Multiple people in frame
- Photo of a photo (not live person)
- Face does not match ID document

Solution:

1. **Show clear instructions before selfie (Norwegian):**

```
Slik tar du et godt selfie-bilde:
✓ God belysning (dagslys er best)
✓ Fjern briller/solbriller
✓ Se rett i kameraet
✓ Kun ditt ansikt i bildet
✗ Ikke bruk foto av foto
```

2. **Allow retry with better instructions:**

```
Selfie-verifisering mislyktes
Prøv igjen med bedre belysning.
Sørg for at ansiktet ditt er tydelig synlig.
```

3. **Improve liveness detection settings (if too strict):**
   - Login: https://cockpit.sumsub.com
   - Navigate to Settings → Verification Levels
   - Adjust liveness sensitivity (low/medium/high)
   - Balance: security vs user friction
4. **Manual review (if automated fails repeatedly):**
   - Some users may need manual review
   - Sumsub team reviews video/photos manually
   - ETA: 1-24 hours depending on Sumsub queue

ETA: Immediate (user retry), 1-24 hours (manual review)

Emergency Workarounds

Option 1: Manual KYC Review (Temporary)

Use case: Sumsub down >1 hour, urgent user needs verification

Steps:

1. Collect KYC documents manually:
   - Ask user to email ID photo + selfie to support@getdrop.no
   - Subject: "KYC Manual Review - [User ID]"
2. **Alem or John reviews manually:**
   - Verify ID document authenticity (check security features)
   - Compare selfie to ID photo
   - Check ID expiry date
   - Verify age >= 18
3. **Manual AML check:**
   - Search user name on: https://sanctionssearch.ofac.treas.gov
   - Check EU sanctions list: https://eeas.europa.eu/topics/sanctions-policy
   - Document findings
4. **Approve in database (if passes checks):**

   ```
   UPDATE users
   SET kyc_status = 'approved_manual',
       kyc_approved_at = datetime('now'),
       kyc_approved_by = 'john',
       kyc_notes = 'Manual review during Sumsub outage'
   WHERE user_id = '<user-id>';
   ```

5. **Notify user:**

   ```
   Din identitet er verifisert
   Velkommen til Drop! Du kan nå gjøre betalinger.
   ```

Risk: Manual review is slow, error-prone, not scalable. Only for critical cases.

Option 2: Delay Registration, Notify When Ready

Use case: Sumsub down, no ETA, non-urgent registrations

Steps:

1. Show maintenance message:

   ```
   Identitetsverifisering midlertidig utilgjengelig
   Vi jobber med å løse problemet.
   Du vil motta en e-post når du kan fortsette registreringen.
   ```

2. Collect user email:

```
// src/app/api/auth/register/route.ts
if (sumsubUnavailable) {
  await db.insert('pending_registrations', {
    email: userEmail,
    status: 'waiting_kyc',
    created_at: new Date(),
  });

  return {
    success: true,
    message: 'We will notify you when registration is available',
  };
}
```

3. **When Sumsub is back, notify users:**

   ```
   SELECT email FROM pending_registrations WHERE status = 'waiting_kyc';
   ```

   Email (Norwegian):

   ```
   Emne: Du kan nå fullføre registreringen i Drop

   Hei,

   Identitetsverifisering er tilbake.
   Klikk her for å fortsette registreringen: [Link]

   Mvh,
   Drop
   ```

ETA: Delayed registration (hours to days)

Monitoring & Alerts

Metrics to Track

- **KYC success rate:** Should be >85% (accounting for user errors)
- **KYC processing time:** p50 <5min, p95 <30min, p99 <2h (includes manual review)

- **Rejection reasons:** Track document_not_readable, expired, underage, sanctions separately

Alert Rules

```
// src/lib/kyc-monitor.ts
export async function trackKYCFailure(userId: string, reason: string) {
  const failureRate = await calculateKYCFailureRate('last_hour');

  if (failureRate > 0.3) { // 30% failure rate
    await sendAlert({
      severity: 'high',
      title: 'KYC failure rate high',
      message: `${(failureRate * 100).toFixed(1)}% of KYC attempts failing`,
      reason,
    });
  }
}
```

Post-Incident Actions

1. **Retry failed KYC verifications:**

   ```
   UPDATE users
   SET kyc_status = 'pending_retry',
       kyc_retry_at = datetime('now')
   WHERE kyc_status IN ('failed', 'pending_kyc')
   AND created_at > datetime('now', '-24 hours');
   ```

2. **Document incident:**

   ```
   touch ~/ALAI/products/Drop/comms/incidents/$(date +%Y-%m-%d)-sumsub-kyc-failure.md
   ```

3. **Review rejection reasons:**
   - High document_not_readable rate? Improve photo instructions
   - High liveness_check_failed rate? Adjust Sumsub settings
   - Track improvements in next month's KYC metrics
4. **Update user onboarding:**
   - Add better photo guides
   - Show example of good vs bad ID photos
   - Pre-flight check: "Is your ID expired?"

Escalation

Time	Action
0 min	John starts diagnosis
15 min	If Sumsub outage confirmed, notify Alem
30 min	If urgent user needs KYC, consider manual review (Alem approval)
1 hour	Public communication to users
2 hours	Contact Sumsub support via phone if no response

Contacts

- **Sumsub Support:** support@sumsub.com
- **Sumsub Live Chat:** https://cockpit.sumsub.com (bottom-right)
- **Sumsub Phone:** Check Sumsub Dashboard for support number
- **Internal:** Alem (CEO, manual KYC approval authority)

Related Documentation

- `docs/architecture/kyc-aml.md` — KYC/AML flow diagrams
- `src/app/api/kyc/initiate/route.ts` — Sumsub integration code
- `docs/compliance/kyc-requirements.md` — Regulatory requirements (age, ID types)
- Vaultwarden item: "Sumsub API" — Credentials

Last Updated: 2026-02-22 **Next Review:** Before Phase 2 (Banking Integration)

Revision #6
Created 2026-02-23 11:29:21 UTC by John
Updated 2026-05-25 07:27:45 UTC by John