Bank Partner Due Diligence Questionnaire

Divy It Up, LLC

Document Creation Date:	March 18th, 2026
Effective Date:	March 19th, 2026
Version:	1.1
Classification:	Public

1. How is sensitive financial data protected?

All sensitive financial data (account numbers, routing numbers, access tokens) is encrypted using AES-256-GCM via an envelope encryption model backed by Amazon Web Services (AWS) Key Management Service (KMS).

- Data is encrypted immediately upon receipt
- No plaintext sensitive data is stored
- Only encrypted values and associated metadata are persisted

---

2. Where are encryption keys stored?

All master keys are stored and managed within AWS KMS

- Keys are HSM-backed
- Key material is not accessible to application systems or personnel
- Application systems only receive temporary data keys for encryption/decryption

---

3. Who has access to decrypt sensitive data?

Only a single backend service role has permission to perform decryption.

- No human users have decrypt access
- Access is restricted via IAM role and KMS key policy
- Role is scoped to specific environments and workloads

---

4. How are credentials managed?

Our back-end Server system uses federated identity (OIDC) to obtain short-lived AWS credentials at runtime.

- No long-lived AWS credentials are stored
- Credentials expire automatically
- Access is granted only after identity verification

---

5. Is encryption applied at rest and in transit?

Yes.

- At rest: Application-layer encryption using AES-256-GCM + KMS
- In transit: TLS 1.2+ for all communications

---

6. How is key rotation handled?

- AWS KMS supports automatic key rotation for customer-managed keys
- Divy It Up rotates keys at least every 60 calendar days.
- Rotated keys remain capable of decrypting previously encrypted data
- Rotation does not disrupt application functionality

---

7. Are cryptographic operations logged?

Yes. All key usage is logged via AWS CloudTrail, including:

- Decryption operations
- Key generation
- Role assumption events

Logs include identity, timestamp, and request metadata.

---

8. How is access restricted to production systems?

Access is restricted through:

- IAM roles with least-privilege permissions
- Environment-scoped trust policies
- Separation of production vs. non-production roles

Only authorized workloads in the production environment can assume the production role.

---

9. Is sensitive data ever exposed to client applications?

No.

- Sensitive values are never returned to client applications
- Only masked values (e.g., last 4 digits) are exposed for display

---

10. How is decrypted data handled?

- Decryption occurs only in memory
- Data is used immediately for required operations
- No decrypted values are persisted or logged

---

11. What protections exist against insider threats?

- No employee has access to raw encryption keys
- No employee has direct decrypt permissions in production
- All access is logged and attributable

- Separation of duties prevents privilege escalation

---

12. How does the system prevent credential leakage?

- No static credentials stored in code or environment
- All access uses short-lived tokens
- Tokens are scoped and automatically expire

---

13. What standards or best practices does this align with?

The architecture aligns with:

- AWS KMS best practices
- Envelope encryption standards
- Least privilege IAM design
- Secure key management principles used in fintech systems
- SOC 2 Security and Confidentiality criteria (see our SOC 2 Control Narrative for more details)

---

14. Do you store raw full bank account and routing numbers?

No, we store encrypted (at rest). When stored:

- Values are encrypted at the application layer
- Only ciphertext is persisted

---

15. Can encryption keys be exported?

No.

- AWS KMS does not allow export of key material
- Keys remain within AWS-managed HSM infrastructure

Closing Positioning Statement

Divy It Up's security architecture is designed to meet the expectations of regulated financial systems by combining:

- Hardware-backed key management (AWS KMS)
- Strong encryption (AES-256-GCM)
- Federated identity with short-lived credentials
- Strict least-privilege access controls
- Full auditability of all sensitive operations

This ensures that sensitive financial data is secure by design, not by convention.