ID Title: SEC-2025-0001 – Negative Transfer Vulnerability
Location: Payment Gateway / Transfer Endpoint
Severity: Critical
Impact: The system currently allows transferring funds with negative amounts, which can bypass balance checks and potentially enable unauthorized withdrawals.

Technical Details

- When intercepting the transfer request and modifying the `amount` field to a negative value, the transaction still completes successfully—even if the source account has a zero or insufficient balance.
- This behavior indicates missing or insufficient server-side validation of transaction amounts.
- It also raises risks of fraudulent or incorrect financial operations, creating inconsistencies in transactional data.

Example Request

```
{
  "sourceAccountId": "SMAJ73030582",
  "recipientId": "3f41f250-1bb6-4b5a-9ecc-a7a4825fa000",
  "description": "Negative transfer test",
  "destinationAccountId": "SMA7J303847",
  "amount": "-78.4"
}
```

Example Response

Sender	Recipient	Amount	Date
Sif Gimrarsdóttir	Sif Gimrarsdóttir	-78.4	2025-02-07T16:56:24.1675882

The transaction is recorded as if it were valid, deducting a negative sum without verifying adequate funds.

Recommendation

1. **Server-Side Validation**: Enforce strict server-side checks to reject negative amounts unless explicitly permitted in special scenarios.
2. **Balance Verification**: Confirm the source account's available balance is sufficient before processing any transfer.
3. **Logging & Alerts**: Log all negative transfer attempts and generate alerts for system administrators to investigate.
4. **Security Controls**: Review and update API security controls, ensuring no tampering can bypass essential validations.

All fixes should be applied immediately to prevent potential exploitation and maintain the integrity of financial transactions.