

# Assure DeFi<sup>®</sup>

THE VERIFICATION **GOLD STANDARD**



## Security Assessment

### VirtueFinance

Date: 12/06/2025

Audit Status:

**PENDING PASS**

Audit Edition: Advanced



ASSURE DEFI<sup>®</sup>  
THE VERIFICATION **GOLD STANDARD**

# Risk Analysis

## Vulnerability summary

Classification	Description
 High	High-level vulnerabilities can result in the loss of assets or manipulation of data.
 Medium	Medium-level vulnerabilities can be challenging to exploit, but they still have a considerable impact on smart contract execution, such as allowing public access to critical functions.
 Low	Low-level vulnerabilities are primarily associated with outdated or unused code snippets that generally do not significantly impact execution, sometimes they can be ignored.
 Informational	Informational vulnerabilities, code style violations, and informational statements do not affect smart contract execution and can typically be disregarded.

## Executive Summary

According to the Assure assessment, the Customer's smart contract is **Poorly Secured**.



# Scope

## Target Code And Revision

For this audit, we performed research, investigation, and review of the VirtueFinance contracts followed by issue reporting, along with mitigation and remediation instructions outlined in this report.

## Target Code And Revision

<b>Project</b>	Assure
<b>Language</b>	Solidity
<b>Codebase</b>	<a href="https://etherscan.io/address/0xbcc711e8ed39b3ca38364f4135571c9877155875#code">https://etherscan.io/address/0xbcc711e8ed39b3ca38364f4135571c9877155875#code</a>
<b>Audit Methodology</b>	Static, Manual

# Attacks made to the contract

In order to check for the security of the contract, we tested several attacks in order to make sure that the contract is secure and follows best practices.

Category	Item
Code review & Functional Review	<ul style="list-style-type: none"><li>• Compiler warnings.</li><li>• Race conditions and Reentrancy. Cross-function race conditions.</li><li>• Possible delays in data delivery.</li><li>• Oracle calls.</li><li>• Front running.</li><li>• Timestamp dependence.</li><li>• Integer Overflow and Underflow.</li><li>• DoS with Revert.</li><li>• DoS with block gas limit.</li><li>• Methods execution permissions.</li><li>• Economy model.</li><li>• Private user data leaks.</li><li>• Malicious Event log.</li><li>• Scoping and Declarations.</li><li>• Uninitialized storage pointers.</li><li>• Arithmetic accuracy.</li><li>• Design Logic.</li><li>• Cross-function race conditions.</li><li>• Safe Zeppelin module.</li><li>• Fallback function security.</li><li>• Overpowered functions / Owner privileges</li></ul>



# AUDIT OVERVIEW



## 1. Re-Entrancy via addLiquidityETH [N/A ✓]

**Function:** \_transfer

**Issue:** No re-entrancy guard on owner's addLiquidity, which calls external router payable function.

**Recommendation:** Add lockSwap-style mutex to addLiquidity, or use OpenZeppelin's ReentrancyGuard.

**Fix:** Only the uniswap router will be used, so the issue is resolved and does not apply.

## 2. Re-opening Trading Abuse [Fixed ✓ - Pending renounce ownership]

**Function:** openTrading

**Issue:** Owner can repeatedly call openTrading, resetting blockLaunch and manipulating anti-bot tax.

**Recommendation:** Restrict openTrading to one-time use or emit event and block further calls.

**Fix:** Ownership will be relinquished once the contract is operational, so the issue will be resolved.



## 1. Dynamic High Tax (80%)

**Function:** \_transfer

**Issue:** Anti-bot logic allows tax >20%, bypassing setTax cap, potentially locking trades.

**Recommendation:** Define a uint256 public conLimit tax with a hardcoded MAX\_ANTI\_BOT\_TAX (for example, ≤80%), add explicit comments, emit an event when it triggers, and document in UI/docs.

## 2. Front-Running & Sandwich Attacks

**Function:** \_transfer

**Issue:** Concentrated swap logic on sells (swapTokensEth) can be MEV-exploited.

**Recommendation:** Randomize swap thresholds or split swaps over blocks; consider time-weighted average pricing.

### **3. Race Condition on Limit Updates**

**Function:** Limit setters

**Issue:** changing maxWallet/maxTransaction in-flight can block user transactions unexpectedly.

**Recommendation:** Emit events on limit changes; consider grace period before new limits take effect.

### **4. Centralized Control & Single Point of Failure [Fixed - Pending renounce ownership]**

**Function:** All admin

**Issue:** Owner and taxAddress hold unilateral power (e.g., modifying exemptions, draining funds).

**Recommendation:** Consider multisig or timelock for sensitive operations; allow taxAddress rotation via governance.

**Fix:** Ownership will be relinquished once the contract is operational, so the issue will be resolved.



#### **1. Parameter Overflow & Revert**

**Function:** triggerSellCA

**Issue:** Multiplying amount \* 10\*\*decimals can overflow and revert.

**Recommendation:** Validate amount bounds before scaling; use SafeCast.

#### **2. Parameter Overflow & Revert**

**Function:** Unchecked Return Value

**Issue:** ERC-20 transfer return value ignored, risking silent failure.

**Recommendation:** Use OpenZeppelin's SafeERC20 to handle transfer return values and revert on failure.



#### **1. Miner manipulation**

**Issue:** Reliance on block.number for anti-bot can be skewed by miners.

**Recommendation:** Consider using block.timestamp or time-based window instead of single block number.

# Technical Findings Summary

## Findings

Vulnerability Level	Total	Pending	Not Apply	Acknowledged	Partially Fixed	Fixed
<div><div></div>High</div>	2		1			1
<div><div></div>Medium</div>	4					1
<div><div></div>Low</div>	2					
<div><div></div>Informational</div>	1					

# Assessment Results

## Score Results

Review	Score
Global Score	85/100
Assure KYC	Not completed
Audit Score	85/100

The Following Score System Has been Added to this page to help understand the value of the audit, the maximum score is 100, however to attain that value the project must pass and provide all the data needed for the assessment. Our Passing Score has been changed to 84 Points for a higher standard, if a project does not attain 85% is an automatic failure. Read our notes and final assessment below. The Global Score is a combination of the evaluations obtained between having or not having KYC and the type of contract audited together with its manual audit.

## **Audit - PENDING PASS**

Following our comprehensive security audit of the token contract for the VirtueFinance project, once the ownership renouncement is made, the project will remain as PASS.



# Disclaimer

Assure Defi has conducted an independent security assessment to verify the integrity of and highlight any vulnerabilities or errors, intentional or unintentional, that may be present in the reviewed code for the scope of this assessment. This report does not constitute agreement, acceptance, or advocating for the Project, and users relying on this report should not consider this as having any merit for financial adVirtueFinance in any shape, form, or nature. The contracts audited do not account for any economic developments that the Project in question may pursue, and the veracity of the findings thus presented in this report relate solely to the proficiency, competence, aptitude, and discretion of our independent auditors, who make no guarantees nor assurance that the contracts are entirely free of exploits, bugs, vulnerabilities or deprecation of technologies.

All information provided in this report does not constitute financial or investment adVirtueFinance, nor should it be used to signal that any person reading this report should invest their funds without sufficient individual due diligence, regardless of the findings presented. Information is provided 'as is, and Assure Defi is under no covenant to audit completeness, accuracy, or solidity of the contracts. In no event will Assure Defi or its partners, employees, agents, or parties related to the provision of this audit report be liable to any parties for, or lack thereof, decisions or actions with regards to the information provided in this audit report.

The assessment serVirtueFinances provided by Assure Defi are subject to dependencies and are under continuing development. You agree that your access or use, including but not limited to any serVirtueFinances, reports, and materials, will be at your sole risk on an as-is, where-is, and as-available basis. Cryptographic tokens are emergent technologies with high levels of technical risk and uncertainty. The assessment reports could include false positives, negatives, and unpredictable results. The serVirtueFinances may access, and depend upon, multiple layers of third parties.