Wishes Fraud Management Program

INTRODUCTION

The FFIEC agencies have provided long-standing guidance on the requirements of financial institutions to have an appropriate risk-based fraud prevention program. Additional guidance has been provided to those institutions offering internet-based products and services. Fraud can be broadly defined as an intentional act of deceit to obtain an unjust/illegal advantage.

Fraud includes any attempt by a customer or a non-customer to obtain Wishes products or services illegally. This may include, but is not limited to, the following:

- Providing inaccurate information to qualify for a product or service;
- Identity theft;
- Providing documentation that is inconsistent with application or account information;
- Falsely disputing transactions;
- Forgery;
- Fraudulent ACH transactions;
- Credit card fraud, such as skimming;
- Account takeover;
- Phishing or internet fraud; and
- Money laundering.

GOVERNANCE AND OVERSIGHT

Senior Management is responsible for oversight of Wishes compliance with the requirements of this policy. Senior Management will formally adopt this policy on at least an annual basis as part of Wishes Compliance Program.

The Board of Directors will remain informed of Wishes compliance with this policy through periodic reporting on the effectiveness of the Compliance Program.

POLICY STATEMENT

It is Wishes policy to ensure appropriate controls are implemented to identify potential fraud; to thoroughly investigate potential fraud; provide reporting on internal and external fraud; and implement corrective action, when required, to mitigate future instances of fraud.

RISK ASSESSMENT

Wishes will review and update fraud risk assessments on a no less than annual frequency and consider the following:

- Changes in the internal and external threat environment;

- Changes in the customer base;
- Changes in the products or customer functionality offered; and
- Actual incidents of security breaches, identity theft and fraud experienced by Wishes or throughout the industry.

IDENTITY THEFT PROGRAM

Financial identity theft occurs when someone uses another consumer's personal information, such as name, social security number, etc. with the intent of conducting transactions to commit fraud that results in substantial harm or inconvenience to the victim. The fraudulent activity may include opening deposit accounts, establishing credit card or line of credit accounts or gaining access to the victim's accounts with the intent of depleting balances. Some other examples of identity theft include account takeover and credit takeover, explained below.

While consumers don't create accounts directly with Wishes, it is possible that a consumer of our business customers becomes a victim of identity theft or account takeover whereby Wishes products or services are used to facilitate fraud. In these instances, Wishes may be included in an investigation of that fraud and required to provide documentation of any transactions.

Additionally, business accounts may be opened under false pretenses in an attempt to commit fraud or money laundering. Wishes conducts appropriate levels of due diligence on business clients and conducts transaction monitoring, as outlined below, to identity these situations.

FRAUD RISK MITIGATION

Mitch Trulli is responsible for ensuring appropriate written procedures and internal controls are adopted and that technology solutions are designed in a way as to ensure compliance with this policy. Internal controls and procedures will be tested at least annually by internal and/or external auditors. Reports of these audits will be provided to management and the Board with recommendations for corrective action.

Layered Security

Layered security is characterized by the use of different controls at different points in a transaction process so that a weakness in one control is generally compensated for by the strength in a different control. Layered security can substantially strengthen the overall security of internet-based services and can be effective in protecting sensitive customer information, preventing identity theft, and reducing account takeovers and the resulting financial losses. Wishes has implemented a layered security program which includes, but is not limited to the following:

- Fraud detection and monitoring systems that include consideration of customer history and
- The use of 2 factor authentication through Twilio

- Enhanced controls over account activities, such as transaction value thresholds, payment recipients, number of transactions allowed per day and allowable payment windows.
- Internet protocol (IP) reputation-based tools to block connection to servers from IP addresses known or suspected to be associated with fraudulent activities;
- Policies or practices for addressing customer devices identified as potentially compromised and customer who may be facilitating fraud;
- Enhanced control over changes to account maintenance activities performed by customers either online or through customer service channels; and
- Enhanced customer education to increase awareness of fraud risk and effective techniques customers can use to mitigate the risk.

Automated Account Monitoring

As part of its system design, Wishes has engaged companies for transaction monitoring, ofac, kyc and kyb reporting and created a special alert to inform users of the system of the need for investigation.
Transaction monitoring may include individual user requests or combination of user requests, such as:

- Large money transfers;
- Abnormal money transfers for individual users;
- Money transfers to new or risky destination accounts;
- Behavior indicative of account takeover such as changing contact address, executing high value transactions, or changing mailing address and then ordering checks or access devices;
- Accessing online banking from an unusual location or at an unusual time of day, such as from a new state or country;
- Login from a new device or computer;
- Using online features not typically used;
- Using online banking features in an unexpected sequence;
- Changing personal information;
- Adding payees or new user/signor; or
- Types and amounts of transactions.

Security Threats

While monitoring of individual transactions is important, progressive fraud attacks may hijack a user's session and mask both the identity and behavior of the user. As part of the fraud prevention policy and procedure, Founder Sass Society has established an **Information Security Policy**, which details specific system controls to prevent unauthorized access to Founder Sass Society systems.

The Information Security Policy is designed to govern controls Founder Sass Society has or will implement to do the following:

- Monitor threat alerts;
- Monitor service availability and diagnose causes of reduced availability;
- Monitor applications and network traffic for indicators of nefarious activity;
- Ensure traffic filtering by Wishes ISP;
- Design and implement applications to withstand application level denial of service (DOS) attacks;
- Utilize distributed architecture;
- Limit traffic; and
- Add bandwidth.

Reporting a Suspected Fraud

Reporting fraud according to the following procedures is mandatory for any employee who suspects fraud has occurred. When dealing with fraud, it is important to avoid the following:

- Alerting suspected individuals that an investigation is underway;
- Making statements that could lead to claims of false accusations or other charges.

Details of the incident, facts, suspicions or allegations should not be discussed with anyone inside or outside of Wishes unless the team investigating the claim requires it. The matter should never be discussed with the individual suspected of fraud.

Internal controls and procedures will be tested at least annually by internal and/or external auditors. Reports of these audits will be provided to management and the Board with recommendations for corrective action, when required.

TRAINING

All appropriate Wishes employees will be provided training on this policy and specifically in recognizing potential identity theft. Additional training will be provided throughout the year, as necessary, if incidents of identity theft or attempted identity theft are uncovered.

REPORTING

Our Team will submit a report to the Board on a no less frequent than annual basis that outlines the changes in risk to customers and to the safety and soundness of Wishes. The report will include the following:

- The effectiveness of the policies and procedures implemented by management;
- Changes in business arrangements, including mergers and acquisitions, joint ventures and service provider arrangements;
- Significant incidents involving attempted or actual identity theft and management's response to the incident(s);
- Recommendations for any changes to the program.

RECORD RETENTION

Wishes will retain all applicable records related to fraud and identity theft investigations for five (5) years.

VERSION CONTROL

Version 2.2 May 13, 2025