



# NAVER FINANCIAL Corporation

## System and Organization Controls 3 Report

On Controls Relevant to Security, Availability, Processing Integrity, Confidentiality, and  
Privacy of  
NAVER Pay Service

January 1, 2023 – December 31, 2023

# Table of contents

- Section I: Independent Service Auditor’s Report .....2
- Section II: Management’s Assertion.....4
- Section II: Management’s Assertion (Subservice Organization) .....5
- Section III: Description of the Boundaries of NAVER Pay Service System .....6
  - 1. Overview of Operations .....6
    - Company Introduction .....6
    - Service .....6
    - Report Scope Boundary .....7
  - 2. Service Components .....7
    - Infrastructure .....7
    - Software.....7
    - Human Resources.....7
    - Procedures .....7
    - Data .....8
- Section IV: Principal Service Commitments and System Requirements .....9

## Section I: Independent Service Auditor's Report

English Translation of Independent Auditors' Report Originally Issued in Korean on April 26, 2024

### NAVER FINANCIAL Corporation

NAVER 1784,  
95, Jeongjail-ro, Bundang-gu,  
Seongnam-si, Gyeonggi-do,  
Korea

### Scope

We have examined NAVER FINANCIAL Corporation ('NAVER FINANCIAL', or the 'service organization')'s accompanying assertion titled "Section II: Management's Assertion" ('assertion') that the controls within the NAVER Pay Service system ('system') were effective and NAVER CLOUD Corporation ('NAVER CLOUD', or the 'subservice organization')'s accompanying assertion titled "Section II: Management's Assertion(Subservice Organization)" ('Subservice Organization's assertion') that the controls designed by NAVER FINANCIAL and operated by NAVER CLOUD were effective throughout the period January 1, 2023 to December 31, 2023, to provide reasonable assurance that NAVER FINANCIAL's service commitments and system requirements were achieved based on the trust services criteria relevant to security, availability, processing integrity, confidentiality, and privacy ('applicable trust services criteria') set forth in TSP Section 100, *2017 Trust Services Criteria for Security, Availability, Processing Integrity, Confidentiality, and Privacy*, in AICPA, *Trust Services Criteria*.

NAVER FINANCIAL uses NAVER CLOUD to IT infrastructure operation service related to NAVER Pay service. The service provided by NAVER CLOUD is part of NAVER Pay service and the controls designed by NAVER FINANCIAL and operated by the subservice organization that are necessary for NAVER FINANCIAL to achieve its service commitments and system requirements based on the applicable trust services criteria.

### Service Organization's Responsibilities

NAVER FINANCIAL is responsible for its service commitments and system requirements and for designing, implementing, and operating effective controls within the system to provide reasonable assurance that NAVER FINANCIAL's service commitments and system requirements were achieved. NAVER FINANCIAL has also provided the accompanying assertion about the effectiveness of controls within the system. When preparing its assertion, NAVER FINANCIAL is responsible for selecting, and identifying in its assertion, the applicable trust services criteria and for having a reasonable basis for its assertion by performing an assessment of the effectiveness of the controls within the system.

### Subservice Organization's Responsibilities

NAVER CLOUD has provided the accompanying assertion about the effectiveness of the controls designed by NAVER FINANCIAL and operated by NAVER CLOUD. When preparing its assertion, NAVER CLOUD is responsible for having a reasonable basis for its assertion by performing an assessment of the effectiveness of the controls designed by NAVER FINANCIAL, which enable NAVER FINANCIAL to achieve its service commitments and system requirements.

### Service Auditor's Responsibilities

Our responsibility is to express an opinion, based on our examination, on management's assertion that controls within the system were effective throughout the period to provide reasonable assurance that the service organization's service

commitments and system requirements were achieved based on the applicable trust services criteria. Our examination was conducted in accordance with attestation standards established by the American Institute of Certified Public Accountants (AICPA) and International Standard on Assurance Engagements 3000, *Assurance Engagements Other Than Audits or Reviews of Historical Financial Information*, issued by the International Auditing and Assurance Standards Board (IAASB). Those standards require that we plan and perform our examination to obtain reasonable assurance about whether management's assertion is fairly stated, in all material respects. We believe that the evidence we obtained is sufficient and appropriate to provide a reasonable basis for our opinion.

We are required to be independent and to meet our other ethical responsibilities in accordance with relevant ethical requirements relating to the engagement.

Our examination included the following:

- Obtaining an understanding of the system and the service organization's service commitments and system requirements
- Assessing the risks that controls were not effective to achieve NAVER FINANCIAL's service commitments and system requirements based on the applicable trust services criteria
- Performing procedures to obtain evidence about whether controls within the system were effective to achieve NAVER FINANCIAL's commitments and system requirements based on the applicable trust services criteria

Our examination also included performing such other procedures as we considered necessary in the circumstances.

## Service Auditor's Independence and Quality Control

We have complied with the independence and other ethical requirements of the *Code of Professional Conduct* established by the AICPA and the *Code of Ethics for Professional Accountants* issued by the International Ethics Standards Board for Accountants, which are founded on fundamental principles of integrity, objectivity, professional competence and due care, confidentiality, and professional behavior. We applied the statements on quality control standards established by the AICPA and International Standards on Quality Management 1, *Quality Management for Firms that Perform Audits or Reviews of Financial Statements, or Other Assurance or Related Services Engagements*, and accordingly maintain a comprehensive system of quality control.

## Inherent limitations

There are inherent limitations in the effectiveness of any system of internal control, including the possibility of human error and the circumvention of controls.

Because of their nature, controls may not always operate effectively to provide reasonable assurance that the service organization's service commitments and system requirements were achieved based on the applicable trust services criteria. Also, the projection to the future of any conclusions about the effectiveness of controls is subject to the risk that controls may become inadequate because of changes in conditions or that the degree of compliance with policies or procedures may deteriorate.

## Opinion

In our opinion, management's assertion that the controls within NAVER FINANCIAL's NAVER Pay Service system were effective throughout the period January 1, 2023 to December 31, 2023, to provide reasonable assurance that NAVER FINANCIAL's service commitments and system requirements were achieved based on the applicable trust services criteria is fairly stated, in all material respects.

*Deloitte Anjin LLC.*

April 26, 2024  
Seoul, Republic of Korea



## Section II: Management's Assertion

We are responsible for designing, implementing, operating, and maintaining effective controls within NAVER FINANCIAL Corporation ('NAVER FINANCIAL' or the 'service organization')'s NAVER Pay service system ('system') throughout the period January 1, 2023 to December 31, 2023, to provide reasonable assurance that NAVER FINANCIAL's service commitments and system were achieved based on the trust services criteria relevant to security, availability, processing integrity, confidentiality, and privacy (applicable trust services criteria) set forth in TSP section 100, *2017 Trust Services Criteria for Security, Availability, Processing Integrity, Confidentiality, and Privacy, in AICPA Trust Services Criteria*. Our description of the boundaries of the system is presented in Section III and identifies the aspects of the system covered by our assertion.

We have performed an evaluation of the effectiveness of the controls within the system throughout the period January 1, 2023 to December 31, 2023, to provide reasonable assurance that NAVER FINANCIAL's service commitments and system requirements were achieved applicable trust services criteria. NAVER FINANCIAL's objectives for the system in applying the applicable trust services criteria are embodied in its service commitments and system requirements relevant to the applicable trust services criteria. The principal service commitments and system requirements related to the applicable trust services criteria are presented in Section IV.

NAVER FINANCIAL uses NAVER CLOUD Corporation ('NAVER CLOUD') to provide IT infrastructure operation service related to NAVER Pay service. The service provided by NAVER CLOUD is part of NAVER Pay service and the controls designed by NAVER FIANANCIAL and operated by the subservice organization that are necessary for NAVER FINANCIAL to achieve its service commitments and system requirements based on the applicable trust services criteria.

There are inherent limitations in any system of internal control, including the possibility of human error and the circumvention of controls. Because of these inherent limitations, a service organization may achieve reasonable, but not absolute, assurance that its service commitments and system requirements are achieved.

We assert that the controls of NAVER FINANCIAL and the controls designed by NAVER FINANCIAL and operated by NAVER CLOUD within the system were effective throughout the period January 1, 2023 to December 31, 2023, to provide reasonable assurance that NAVER FINANCIAL's service commitments and system requirements were achieved based on the applicable trust services criteria.



## Section II: Management's Assertion (Subservice Organization)

NAVER CLOUD Corporation ('NAVER CLOUD' or 'we') provides IT infrastructure operation service related to NAVER Pay service to NAVER FINANCIAL Corporation ('NAVER FINANCIAL'). The service provided by NAVER CLOUD is part of NAVER Pay service. We are responsible for the operating effectiveness of controls designed by NAVER FINANCIAL within NAVER Pay Service system ('system') throughout the period January 1, 2023 to December 31, 2023, to provide reasonable assurance that NAVER FINANCIAL's service commitments and system requirements were achieved based on the trust services criteria relevant to security, availability, processing integrity, confidentiality, and privacy (applicable trust services criteria) set forth in TSP section 100, *2017 Trust Services Criteria for Security, Availability, Processing Integrity, Confidentiality, and Privacy, in AICPA Trust Services Criteria*.

We assert that the controls designed by NAVER FINANCIAL and operated by NAVER CLOUD were effective throughout the period January 1, 2023 to December 31, 2023 based on the applicable trust services criteria.

# Section III: Description of the Boundaries of NAVER Pay Service System

## 1. Overview of Operations

### Company Introduction

NAVER FINANCIAL Corporation ('NAVER FINANCIAL' or the 'Company') was established through spin-off from NAVER Corporation on November 1, 2019 to enhance independence of, and accelerate its initiatives for financial services. NAVER FINANCIAL provides the 'NAVER Pay' service.

Since being officially launched in June 2015, the NAVER Pay Service, which enables users to do shopping at a variety of online stores and pay for various digital contents such as NAVER Music, movies, e-books, etc., recharge and accumulate points, and transfer money using their NAVER IDs, has expanded NAVER's business landscape to simple payment and integrated payment services and been generating synergies leveraging its connection with other existing services.

In 2018, the Company started to support the ZeroPay which is intended to lower burdens of credit card settlement charges for the small businesses and to raise benefits for consumers. The Company started the offline QR payment service together with LINE Pay in Japan to expand its service area to offline.

Starting with the launch of NAVER PAY member-only account service in June 2020, various online financial platform businesses have been prepared so that users can access financial services such as insurance and loan services more conveniently.

In 2021, by utilizing the user data and data-based technology accumulated over the years, the alternative credit rating system was advanced, and the financial platform services were expanded, such as launching the fastest settlement system in the world and the deferred payment service designated as an innovative financial service. It is evolving into a comprehensive financial platform by converting 'My Asset Service' to the MyData API (Application Programming Interface) system and launching the NAVER Pay app.

In addition, in 2022, NAVER FINANCIAL provides extraordinary services through the launch of MyData-based integrated insurance inquiry service and business loans comparison service as the first Fintech company, and it launched Naver Pay Watch App for smartwatches and Naver Pay Hana Bankbook.

In 2023, the Company launched Naver Pay x Samsung Pay MST based on-site payment services and is evolving into innovative financial services by opening on-site payment available in 65 overseas regions/countries and the first simple deposit sign-up/parking account comparison service in fintech.

### Service

NAVER FINANCIAL provides services through PC web and mobile for the users convenience. To deliver such services, NAVER FINANCIAL uses various IT systems, security devices, and internally developed service management systems. The system description covers NAVER Pay service.

NAVER Pay – Allows users to shop, pay, and manage shipments with a single NAVER ID at various affiliate stores, and pay for digital contents such as NAVER Music, Movie, and WebToon.

Users of the service are responsible to adhere to the user's obligation in the Terms of Service in order to securely and properly use the NAVER FINANCIAL services. Users should also understand and perform the activities to protect personal information by themselves, including changing passwords on a regular basis and not disclosing passwords to others.

## Report Scope Boundary

The objective and scope of this description is limited to the NAVER Pay service and does not include any description related to other services.

## 2. Service Components

The Company's service components to provide the service consist of infrastructure, software, data, and relevant operating procedures and human resources.

### Infrastructure

The Company implements and operates infrastructures such as servers, network, and security systems, which are configured in a separate network for each, to provide the service. The Company restricts unauthorized access (physical / logical) using access controls to infrastructure, and monitors the log of abnormal activities on a regular basis.

The Company also uses automatic vulnerability scanning tools to consistently detect and improve security vulnerabilities which may occur within the infrastructure, and takes remedial actions for identified vulnerabilities. The data center, where the infrastructures are located, is equipped with thermo-hygrostats, Uninterruptible Power Supplies (UPS), water leakage detectors, fire detectors, extinguishers, and so on to get prepared for disasters such as fire, earthquake, flood, and so on.

### Software

Relevant functions of the Company for each service are responsible for developing and operating applications. When an application needs additional developments or upgrades to improve service quality provided to users, to remediate failures or to enhance system performance, the security requirements are defined by an agreement between the Service Planning Department and the Development Department and then shared with stakeholders via intranet.

Changes to an application requires preapproval by the person in charge, and the QA (Quality Assurance) team reviews and deploys to the production environment through the automated system to minimize the failures that may arise from the change. When significant changes related to the user's personal information processing are involved, a privacy impact assessment is conducted and remedial actions are taken when deemed necessary.

### Human Resources

To ensure service stability, the Company defines and designates such roles as information security and personal information managers, service planners, developers, infrastructure operators, CS (Customer Satisfaction) personnel, and so on. Annual information security and personal information protection trainings are provided to raise the awareness level of information security of the company personnel.

Immediately after being hired or terminated, an employee is informed of his or her confidentiality obligations, and required to sign and submit a security pledge. All employees sign and submit a security pledge every year.

### Procedures

The Company established information security regulations such as policies, standards and guidelines to comply with the security, availability, process integrity, confidentiality, and privacy principles. Company policies are periodically reviewed, and revised when deemed necessary, to reflect developments of relevant laws and regulations. Revisions require approval by an appropriate level of management and are announced to all employees through intranet.

Company policies related to protection of user's personal information and privacy are disclosed in the Privacy Policy on the Company's website so that users can refer to at any time.



## Data

Important data including user's personal information are protected in accordance with the requirements by relevant laws and regulations such as the Act on Promotion of Information and Communications Network Utilization and information Protection, etc., the Personal Information Protection Act, and so on and the procedures specified in the Terms of Service and security policies of the Company. Such data are managed to be processed only by a limited number of personnel performing relevant duties.

The Company also implements technical measures such as access control, encryption and logging to protect important data.

## Section IV: Principal Service Commitments and System Requirements

The Company has made service commitments to the users and established system requirements for the NAVER Pay service. Some of these commitments are related to the performance of the service and applicable trust services criteria. The Company is responsible for its service commitments and system requirements and for designing, implementing, and operating effective controls within the system to provide reasonable assurance that the Company's service commitments and system requirements are achieved.

Service commitments to users are documented in such forms as Terms of Service, Privacy Policy, Youth Protection Policy, Spam Mail Policy, Search Result Collection Policy, and so on, and communicated to users through the Customer Center. The Company also provides the description of the service offering through online. Service commitments include, but are not limited to, the following:

- **Security:** The Company made commitments related to protecting user data from unauthorized access and use. These commitments are addressed through measures including data encryption, authentication mechanisms, access controls, physical security, and other relevant security controls.
- **Availability:** The Company made commitments related to keeping service continuity without disruptions. These commitments are addressed through measures including performance monitoring, regular data backups and recovery controls.
- **Processing Integrity:** The Company made commitments related to processing user data completely, accurately and timely. These commitments are addressed through measures including secured system development and production environments, approval of system changes and other relevant controls.
- **Confidentiality:** The Company made commitments related to maintaining the confidentiality of user data. These are addressed through security controls including encryption mechanisms in transferring and storing users' important data.
- **Privacy:** The Company made commitments related to protecting personal information. These commitments are addressed through controls relating to collecting, storing, using, entrusting, and disposing of personal information in accordance with relevant laws and regulations and its Privacy Policy.

The Company has established operational requirements that support the achievement of service commitments, requirements by relevant laws and regulations, and other system requirements. Such requirements are specified in the Company's policies and procedures and system design documentation and communicated to users through the service website.

Information security policies of the Company define an organization-wide approach to how systems and data are protected. These include policies over service design and development, system operation, internal business system and network management, and hiring and training of executives and employees. In addition to these policies, standard operating procedures have been documented on how to carry out manual and automated processes specifically required in the operation and development of the NAVER Pay service.