By the Banking Regulation and Supervision Agency:

COMMUNIQUÉ ON MANAGEMENT AND SUPERVISION OF INFORMATION SYSTEMS OF FINANCIAL LEASING, FACTORING AND FINANCING COMPANIES

SECTION ONE

Objective, Scope and Definitions

Objective and Scope

ARTICLE 1 – (1) The objective of this communique is to set down the procedures and principles regarding the management of the information systems and its audit by the authorized independent audit institutions which Leasing, Factoring and Finance Companies use in performing the activities within the scope of the Law.

Basis

ARTICLE 2 – (1) This Communiqué is prepared and issued in reliance upon Article 14(2) of the Financial Leasing, Factoring and Finance Companies Law and the Article 14 of the Regulation on the Establishment and Operating Principles of Financial Leasing, Factoring and Financing Companies, published in the Official Gazette edition 28627 on 24/04/2013.

Definitions and Abbreviations

ARTICLE 3 – (1) The following terms used in this Communique shall have the meanings expressly designated to them below:

a) Explicit consent: Explicit consent defined in the Personal Data Protection Law no. 6698, dated 24/3/2016,
b) Primary systems: The systems in which the information related to the issues in the Law are stored in an electronic environment in a safe and secure manner and allowing access at any time, and the entire system consisting of infrastructure, hardware, software and data used in carrying out the activities,
c) RBISA: Regulation on Information Systems Audit to be performed in Banks by External Audit Institutions published in the Official Gazette dated Jan 13, 2010 and Nr. 27461,
d) Audit trail: Record that enables a financial or operational transaction to be trailed from the beginning until the end,
e) External Service: All kinds of service procurements that organizations provide for information systems,
f) Secondary center: The structure in which secondary systems are established in a way to be available for use and which enables the personnel to operate in an uninterrupted manner and in a way not to hold the same risks as the primary center,
g) Secondary Systems: primary system backups that enable these activities to be maintained within the acceptable deduction periods determined in the information systems continuity plan and to access information related to the issues in the Law in the case of an interruption in activities carried out through primary systems,
h) Law: The Financial Leasing, Factoring and Financing Companies Law No. 6361,
i) PO: Public Oversight, Accounting and Auditing Standards Authority,
j) Control: Control defined in Article 4 of RBISA,
k) Board: Banking Regulation and Supervision Board,
l) Agency: Banking Regulation and Supervision Agency,
m) Penetration test: Attacks realized in order to determine and correct security deficits of the system before being abused,

n) Company: The company defined in Article 3 of the Law,
o) Senior management: Board of directors, general manager and deputy general managers and the managers of units who work in positions equal to or above the deputy general manager in terms of their authorities and duties even if they are employed with other titles, except the consultancy unit's manager

SECTION TWO

Principles for Management of Information Systems

Management of Information Systems

ARTICLE 4 – (1) The company establishes an information systems management structure approved by the board, where corporate governance principles are applied. The company's strategy with regards to information systems is provided to be in line with its business objectives. Necessary financing and human resources are assigned for the security and management of information systems.

(2) The company establishes its policies, procedures and processes regarding information systems for this purpose. Policies, procedures and processes are reviewed and updated regularly. It is ensured that policies, procedures and processes de facto function. In this context, process owners, their responsibilities and control points are defined to ensure the functioning. The controls required for the information systems to provide the services expected of them in a timely, accurate and reliable manner are determined and the effectiveness of these controls is ensured.

(3) Necessary processes and infrastructures are established to control, monitor and ensure undeniability of transactions performed using information systems.

(4) The internal control unit of the company prepares a legislative compliance assessment report, also including issues regarding compliance with policies and procedures, to be submitted to the board of directors once a year.

Risk Management of Information Systems

ARTICLE 5 – (1) The Company creates a risk management process approved by the senior management to identify, analyze, measure, monitor and report risks which stem from the use of information technologies in its activities. The company reviews the risks by follows up and updates them. Within the scope of the process, the company makes evaluations regarding the threats against the assets in the inventory prepared in accordance with the first paragraph of Article 10 of the Communiqué, the probability of occurrence of the risk, the possible consequences that may arise in the event of the risk and measures that can be taken. In the risk analysis to be carried out by the company, regarding each risk identified; it chooses one of the methods such as risk reduction, risk avoidance, acceptance or transfer of risk

(2) While making a risk assessment, the company takes into account the technology infrastructure, the application architecture, criticality of the data kept on the system, risks that may arise from external service providers and technological developments. The risks, which threatening the security and confidentiality of user information, are taken into consideration in the risk assessment.

(3) The company assesses possible risks before significant changes in information systems; take precautions to prevent data loss, service interruption and added risk.

(4) The company ensures the preparation of a risk assessment report that includes the predicted risks and threats regarding the information systems to be submitted to the top-level management once a year.

Information Security Management

ARTICLE 6 – (1) The company establishes the process for information security. The process, roles and responsibilities regarding information security are determined within the board approved Information Security Policy.

(2) The company establishes precautions that provides confidentiality, integrity and accessibility of information systems and data.

(3) The company classifies the data that is acquired, stored, conveyed, and processed on information systems according to their security sensitivity degrees and establishes appropriate level of security control for each class.

(4) The company establishes network control security systems for threats that may come from external networks while communicating with networks outside of its corporate network. The company uses one or more firewalls that are properly configured to control access to the internal network from the external network and to provide a controlled transition by separating the sub-sections of the internal networks which have different security sensitivity.

(5) The company takes the necessary precautions against an external cyber-attack and has a penetration test every 2 years.

(6) The company informs or perform studies that will increase the awareness of the personnel about information security.

(7) The company provides the preparation of a security violation report including unauthorized access attempts, compliance with the information security process and events regarding to information security violation to be submitted to the board of directors once a year.

Authorization and access control

ARTICLE 7 – (1) The company establishes an appropriate authorization and access control for accessing databases, applications and systems. The most limited authority and access rights are granted by taking into account the duties and responsibilities. Authorizations and access rights are reviewed at least once a year in terms of minimum authorization. Only the users, parties and systems who have necessary authorization are granted access to the system, service and data.

(2) The company records and reviews unauthorized access attempts to databases, applications and systems.

(3) The company ensures that the development, testing and production environments are kept separate from each other according to the segregation of duties principal during the design, development, testing and maintenance of the services it offers. Processes and systems are designed and operated in such a way that they do not allow a single person to enter, authorize and complete a critical operation.

(4) For temporary authorizations, the conditions and the period under which this authorization will be given is determined. Additional audit record is kept regarding the temporary authorization.

(5) If the assignment of the employees working within the company or the external service provider end, all their authorizations are terminated immediately.

Authentication

ARTICLE 8 – (1) An appropriate authentication mechanism is established for transactions on information systems taking into consideration the type, characteristics of the transactions, losses that may occur in case of a violation, the type of transaction and the degree of sensitivity of the data. The use of the same user account by more than one person is prevented.

(2) The validity period, complexity and length of the passwords to be used in authentication are ensured to be compatible with the today's technology and the characteristics of the transaction.

(3) The company ensures undeniability in authentication. It takes the necessary precautions towards the confidentiality and security of the authentication information of all users. Critically important data such as passwords are stored in encrypted form or using mathematically irreversible methods in accordance with today's technology, encrypted when transferred and secured against unauthorized access.

(4) The default passwords which are used during hardware and software installation, are changed. New passwords are securely stored.

(5) If failed authentication attempts exceed a certain number, access is blocked and no unnecessary information is given such as the blockage stem either from a username or a password error.

(6) Multiple logins using the same username is prevented and the user is warned that they are logged in more than once in authentication except for those previously allowed. The session is ended in the case of inactivity for a certain period of time.

(7) The authentication to be performed during the remote access of the personnel in the external service providers to the company systems is done by providing at least the same level of security as the company personnel.

Establishing audit trails

ARTICLE 9 – (1) An effective audit trail mechanism regarding to the company's activities is established. Log records are kept while accessing, inquiring the information about company activities and customers, regarding to the authorized access or changing authorization and unauthorized access attempts for these.

(2) The inquiries about sensitive data and personal data held by institutions / organizations through web services, application programming interface or similar methods of the company and the trail records regarding the purpose of these inquiries are also covered by the audit trail. The company takes the necessary precautions to prevent the use of the data it inquires beyond its intended purpose.

(3) It is essential that audit trails are kept in a reportable format and in such a way as not to allow its integrity to be damaged or changed. Audit trails, regarding the transaction; it includes detailed information such as date, time, application information, user name, what information is inquired and changed.

(4) The techniques are used to prevent stopping the audit trail recording system or to detect this situation if stopped.

(5) Access to the systems and databases with privileged or administrator accounts are taken under control and additional trail records are kept. In systems where audit trails are kept, no user including administrators are allowed to make changes on the records.

(6) Audit trails are kept ready for inspection for a minimum of 3 years, save for the derogations provided for other legal provisions related to information and document retention and they are ensured that they are accessible after a possible disaster by taking a backup.

(7) The company ensures that the audit trails kept by the external service provider comply with their standards and that the audit trails are accessible by them within the scope of the service received from the external service provider.

Management of information systems assets

ARTICLE 10 – (1) A process is established regarding the management of hardware, software and data, which are the elements of information systems. The company creates its information systems asset inventory within the framework of:

a) Hardware Inventory: Hardware inventory includes all physical devices and magnetic media that contain company information, which enable it to be displayed, transmitted, and printed regardless of whether it is connected to the corporate network. Personal devices used by personnel to access corporate resources and take action are also included in the inventory. As a minimum, the inventory includes, the type, brand, model, purchase date, date of entry and exit from the inventory, physical location, the applications on it, the authority to make configuration or other changes and ownership information, whether there is availability of backup, information criticality level.
b) Software Inventory: Software inventory includes all software, which used institutionally and located on company hardware, regardless of whether it actively serves or not. Software services used remotely by the company and relevant applications on personal devices used to access institutional resources are also included in the inventory apart from this software services. As a minimum, the inventory contains, the version, the data it accesses, the hardware it works on, the development environment, the criticality level of information.
c) Data Inventory: Data inventory includes the data within the scope of the company's activities on information systems. As a minimum, the information is included in the inventory such as database, whether backup is taken or not, logical address of the backup, the applications using data, who can access it, the level of critical data.

(2) Information systems asset inventory is kept up to date, inventory records of the last 3 years are kept. Necessary precautions are taken to ensure that the equipment removed from the inventory does not carry information about the company.

(3) The company updates the software on information systems. Current patches are followed by establishing a process related to patch management for this. Previous versions of the software that is used are stored securely.

(4) The software used in the production environment is provided to be the same with the version tested and approved in the test environment and changes in the production environment is carried out with the approval of the relevant manager. For this purpose, access to the production environment is restricted, the permissions, which are given temporarily are recorded. Software and database changes are recorded by making it traceable, manual intervention is minimized.

(5) In order to ensure the physical security of the company's information systems;

a) It ensures the security of the area where the information systems are located, takes necessary precautions to protect the area from internal and external threats.
b) Entries and exits to the system room are taken under control, information about entry and exit including information about identifying the person are recorded.

c) It makes monitorable the primary, secondary system rooms and entrances by camera. It preserves the relevant records for at least 6 months.

Information systems continuity plan

ARTICLE 11 – (1) The company prepares an information systems continuity plan approved by the board of directors aiming to ensure the continuity of information systems services that support its activities and important business functions.

(2) Acceptable duration of interruption for each service is determined by assessing the importance level of information systems assets during the preparation of the plan and recovery procedures are developed to enable services to be accessible again in the meantime.

(3) Responsible officers for relevant information systems components and business officers are specified in the plan. The recovery and return steps that need to be applied and the conditions under which these steps will be implemented are defined.

(4) The plan reviewed and updated after events or changes that affect the company's information systems continuity or every year and approved by the board of directors.

(5) Secondary center is established within the scope of the plan. The data and system backups are kept ready to use at the secondary center.

(6) Tests are done at least once a year through the secondary center to ensure the effectiveness and timeliness of the plan, if available, external service providers are included in the tests, test results are reported to the board of directors and the plan is updated according to these results.

External service procurement and management

ARTICLE 12 – (1) Being able to procure external service of information systems is only possible where the decision making and responsibility for functions is on the company for the fulfillment of the duties and responsibilities stemming from the law and the law-related sub-regulations such as management, content design, access, control, audit, updating, reporting.

(2) Regarding the procurement of external services within the scope of information systems, the company's senior management evaluates the risks that the company will pose to implement such services. In this context, the senior management evaluates the level of service, quality and security controls, and the financial structure of the company in accordance with the content of the service implemented.

(3) At the minimum level the company follows the following principles regarding external service procurement related to information systems:

a) Ensuring that all systems and processes comply with the company's own risk management, security and privacy policies,
b) Determination of the ownership and intellectual property rights of the contractual products and services,
c) Providing that the provisions, which constitute obligations for external service providers, are binding in contracts as well to be made with subcontractors,
d) Managing the risks stem from the termination or interruption of external service procurement out of the planned schedule,

e) Ensuring that the provisions of the legislation to which company is subject are also applied to external service providers within the framework of the service received and the necessary changes to be made within the stated period on the company's information systems via the instruction of the Board or Agency,
f) Provisions regarding the transfer of external service to the subcontractor is subject to the permission of the company, restriction of the transfer of external service to a subcontractor without risk assessment and the written permission of the company
g) Ensuring that the external services are subjected to the same level of inspections as in an indepent audit if they are to be performed within the company without narrowing down the scope,
h) External service providers are obligated to provide all kinds of information and documents submitted on time and correctly requested by the Agency and to have and operate the records in all kinds of electronic, magnetic and similar environments related to these, and to access and record all the systems and passwords necessary to make these records readable.

(4) The company establishes the necessary controls for the access of external service providers. Accesses provided for data and system security, given access rights and established controls are regularly reviewed.

(5) The company can use cloud computing services as an external service. Cloud service for primary and secondary systems, can be obtained through a private cloud service model through hardware and software resources allocated to a sole company. In addition to this, it is subject to the permission of the Agency to obtain external services only by means of a group cloud service model by making a logical distinction between the hardware and software allocated to companies' subject to the supervision of the Agency. Furthermore, it is also subject to the permission of the Agency to use a logical distinction between the companies on the hardware and software together with the main partner, its subsidiary and the main partner of a company subject to the Law.

(6) The company is obliged to take necessary precautions in order to ensure the security of confidential information pertaining to the company, its users and customers in the external service procurement. Authorization access given to external service providers is limited to cover the information required by the work. It is the company's responsibility to ensure that precautions are taken by the external service provider to protect confidential information about the company and its users.

Transaction information confidentiality

ARTICLE 13 – (1) The company establishes policies, procedures related to the confidentiality and security of the customer information and the transaction info that is acquired, processed, transmitted or stored and takes necessary precautions.

(2) Except for the parties authorized by the Law, the Company may retain all kinds of information and documents belonging to its customers. Without the explicit consent of the person, it cannot be used for purposes other than the purposes for which it was collected, or for use cannot be passed on to anyone else.

(3) A service to be provided by the company cannot be conditional upon the direct consent of the customer to share information and documents.

SECTION THREE

Independent Audit of Information Systems and Miscellaneous Provisions

Independent audit of information systems

ARTICLE 14 – (1) Information systems audit is a process consisting of stages on forming an opinion on information system elements such as activities, processes, software and hardware within the scope of information systems management in order to determine the compliance of the company with the provisions of this Communiqué. and the effectiveness, on forming an opinion about adequacy and compliance of internal controls, as a result of the evaluation of those internal controls established within these systems and processes by independent audit firms and linking the results to the report.

(2) Information systems audit of the company and reporting of audit results to the Authority, limited to the definition in the first paragraph, is carried out by the independent auditor within the framework of the procedures and principles determined in the fifth section of the RBISA related to the audit in accordance with the standards set by the PO. In the application of this paragraph, the condition in the second paragraph of article 27 of RBISA is not sought.

(3) While the procedures and principles determined by RBISA are applied within the framework of this Communiqué, the expressions “bank” and “audited” refer to the company, “information systems audit” implies to the audit defined in the first paragraph of this article, and the “law” refers to the Law defined in this communiqué.

(4) The independent auditor examines how the company's outsourced services affect the information systems, according to that review if necessary include service providers in the audit and develops an effective audit approach.

(5) Information systems audits are conducted every three years in the company. The Agency is entitled to determine the company to be audited, the year (period) of the audit and the date on which the reports will be submitted. The Agency may diversify the scope and frequency of information systems audit when it considers necessary.

(6) Establishment of audit opinion and audit letter; as a result of the audit carried out in the company, within the framework of the provisions indicated in the 5th and 7th articles of RBISA and the types of opinions specified in the 34th article; in case of positive, conditional or negative opinion, an audit letter is issued in accordance with the examples in Annex-1, Annex-2, Annex-3 respectively. In the case of conditions that would require avoiding expressing an opinion, the audit letter is issued in accordance with the example in Annex-4.

Miscellaneous Provisions

ARTICLE 15 – (1) Within the scope of internet services offered by the company, the company establishes a structure;

a) Guaranteeing that the platform on which the customer carries out transaction belongs to the company,
b) Providing the necessary authentication mechanism in accordance with the risks of the transaction,
c) Informing users about security risks

(2) The company encloses its primary and secondary systems domestically. Within this framework, the information systems used by the external service provider in carrying out the activities related to the respective service and all their backups are kept domestically in case of external service procurement.

SECTION FOUR

Final Provisions

Transition Process

PROVISIONARY ARTICLE 1 — (1) The company shall align its present activities and systems with the provisions of this Communiqué, within maximum one year after the date of promulgation.

Entry into Force

ARTICLE 16 – (1) This Communiqué enters into force on the date of promulgation.

Enforcement

ARTICLE 17 – (1) The provisions of this Communiqué are enforced by the Chairman of Banking Regulation and Supervision Agency.

ANNEX-1

INFORMATION SYSTEMS AUDIT REPORT

Affirmative Opinion

…….. Inc. To the Board of Directors:

As of …../…../…., we have been tasked with controlling information systems of ……... Inc. within the scope of the Communiqué on Management and Control of Information Systems of Financial Leasing, Factoring and Financing Companies.

[Disclosure for the Board of Directors' Responsibility]

It is the responsibility of ……... Inc. Board of Directors to ensure that controls on information systems are established, operated effectively, and an adequate control environment is established in accordance with the procedures and principles set out in the Communiqué on the Management and Control of Information Systems of Financial Leasing, Factoring and Financing Companies.

[Disclosure for the Responsibility of the Authorized Audit Firm]

Our responsibility as an independent auditor, is to deliver an opinion based on our audit work. The audit we have conducted has been planned in a way to provide reasonable assurance to detect important control deficiencies on the auditee's information systems and it was implemented in accordance with the procedures and principles specified in the Communiqué on Management and Control of Information Systems of Financial Leasing, Factoring and Financing Companies. Audit includes testing and evaluating information systems and controls on these systems within the framework of compatibility and the principle of materiality on design and operating efficiency implementation of other similar audit techniques as far as we need. We believe that the audit provides a reasonable and sufficient basis for our opinion.

[Inherent Constraints]

There may be weaknesses of control on information systems due to the inherent restrictions of controls and may not be identified. Besides, the results obtained relied on our findings should not be evaluated in a sense to comprise the future periods. There is a risk that these results will change over time due to the reasons of changes in existing conditions, changes in systems or controls, or deterioration of the degree of effectiveness of the controls.

[Independent Auditor's Opinion]

In our opinion, with all its important parties, ... Inc.'s as of …../…../…. adequate and compatible controls have been established in accordance with the procedures and principles set out in the Communiqué on Management and Control of Information Systems of Financial Leasing, Factoring and Financing Companies

Editing Place and Date of the Report

Responsible Information Systems Lead Auditor

Name and Surname, Signature

Commercial Title of the Organization

ANNEX-2

INFORMATION SYSTEMS AUDIT REPORT

Qualified Opinion

…….. Inc. To the Board of Directors:

As of …../…../…., we have been tasked with controlling information systems of …….. Inc. within the scope of the Communiqué on Management and Control of Information Systems of Financial Leasing, Factoring and Financing Companies.

[Disclosure for the Board of Directors' Responsibility]

It is the responsibility of …….. Inc. Board of Directors to ensure that controls on information systems are established, operated effectively, and an adequate control environment is established in accordance with the procedures and principles set out in the Communiqué on the Management and Control of Information Systems of Financial Leasing, Factoring and Financing Companies.

[Disclosure for the Responsibility of the Authorized Audit Firm]

Our responsibility as an independent auditor, is to deliver an opinion based on our audit work. The audit we have conducted has been planned in a way to provide reasonable assurance to detect important control deficiencies on the auditee's information systems and it was implemented in accordance with the procedures and principles specified in the Communiqué on Management and Control of Information Systems of Financial Leasing, Factoring and Financing Companies. Audit includes testing and evaluating information systems and controls on these systems within the framework of compatibility and the principle of materiality on design and operating efficiency implementation of other similar audit techniques as far as we need. We believe that the audit provides a reasonable and sufficient basis for our opinion.

[Inherent Constraints]

There may be weaknesses of control on information systems due to the inherent restrictions of controls and may not be identified. Besides, the results obtained relied on our findings should not be evaluated in a sense to comprise the future periods. There is a risk that these results will change over time due to the reasons of changes in existing conditions, changes in systems or controls, or deterioration of the degree of effectiveness of the controls.

(Restrictions on independent audit activity and therefore processes, practices, controls that cannot be controlled; lack of substantial controls detected on the auditee's information systems and the main reasons and justifications for the opinion of these control inadequacies not regarding to ffect the whole or most part of information systems.)

[Independent Auditor's Opinion]

In our view, due to the issue (s) described above (in paragraph ....), with all its important parties, except for the possible effects of this issue (s) on the information systems of the audited, ... Inc.'s as of …../…../…. effective, sufficient and compatible controls have been established on information systems in accordance with the principles and procedures set out in the Communiqué on Management and Control of Information Systems of Financial Leasing, Factoring and Financing Companies.

Editing Place and Date of the Report

Responsible Information Systems Lead Auditor

Name and Surname, Signature

Commercial Title of the Organization

ANNEX-3

INFORMATION SYSTEMS AUDIT REPORT

Adverse Opinion

…….. Inc. To the Board of Directors:

As of …../…../…., we have been tasked with controlling information systems of ……... Inc. within the scope of the Communiqué on Management and Control of Information Systems of Financial Leasing, Factoring and Financing Companies.

[Disclosure for the Board of Directors' Responsibility:]

It is the responsibility of ……... Inc. Board of Directors to ensure that controls on information systems are established, operated effectively, and an adequate control environment is established in accordance with the procedures and principles set out in the Communiqué on the Management and Control of Information Systems of Financial Leasing, Factoring and Financing Companies.

[Disclosure for the Responsibility of the Authorized Audit Firm:]

Our responsibility as an independent auditor, is to deliver an opinion based on our audit work. The audit we have conducted has been planned in a way to provide reasonable assurance to detect important control deficiencies on the auditee's information systems and it was implemented in accordance with the procedures and principles specified in the Communiqué on Management and Control of Information Systems of Financial Leasing, Factoring and Financing Companies. Audit includes testing and evaluating information systems and controls on these systems within the framework of compatibility and the principle of materiality on design and operating efficiency implementation of other similar audit techniques as far as we need. We believe that the audit provides a reasonable and sufficient basis for our opinion.

[Inherent Constraints:]

There may be weaknesses of control on information systems due to the inherent restrictions of controls and may not be identified. Besides, the results obtained relied on our findings should not be evaluated in a sense to comprise the future periods. There is a risk that these results will change over time due to the reasons of changes in existing conditions, changes in systems or controls, or deterioration of the degree of effectiveness of the controls.

(reasons of controls are not effective, sufficient or compatible on the information systems of the audited)

[Independent Auditor's Opinion]

In our opinion, with all its significant parties, ... Inc.'s as of …../…../…. compatible controls have not been established in accordance with the procedures and principles stated in the Communiqué on Management and Control of Information Systems of Financial Leasing, Factoring and Financing Companies.

Editing Place and Date of the Report

Responsible Information Systems Lead Auditor

Name and Surname, Signature

Commercial Title of the Organization

ANNEX-4

INFORMATION SYSTEMS AUDIT REPORT

Disclaiming an Opinion

…….. Inc. To the Board of Directors:

As of …../…../…., we have been tasked with controlling information systems of ……... Inc. within the scope of the Communiqué on Management and Control of Information Systems of Financial Leasing, Factoring and Financing Companies.

[Disclosure for the Board of Directors' Responsibility:]

It is the responsibility of ……... Inc. Board of Directors to ensure that controls on information systems are established, operated effectively, and an adequate control environment is established in accordance with the procedures and principles set out in the Communiqué on the Management and Control of Information Systems of Financial Leasing, Factoring and Financing Companies.

[Disclosure for the Responsibility of the Authorized Audit Firm:]

Our responsibility as an independent auditor, is to deliver an opinion based on our audit work. The audit we have conducted has been planned in a way to provide reasonable assurance to detect important control deficiencies on the auditee's information systems and it was implemented in accordance with the procedures and principles specified in the Communiqué on Management and Control of Information Systems of Financial Leasing, Factoring and Financing Companies. Audit includes testing and evaluating information systems and controls on these systems within the framework of compatibility and the principle of materiality on design and operating efficiency implementation of other similar audit techniques as far as we need. We believe that the audit provides a reasonable and sufficient basis for our opinion.

[Inherent Constraints:]

There may be weaknesses of control on information systems due to the inherent restrictions of controls and may not be identified. Besides, the results obtained relied on our findings should not be evaluated in a sense to comprise the future periods. There is a risk that these results will change over time due to the reasons of changes in existing conditions, changes in systems or controls, or deterioration of the degree of effectiveness of the controls.

(Reasons of the auditor did not express an opinion)

[Independent Auditor's Opinion]

Due to the issue (s) described above (in paragraph ...) ..... Inc.'s as of …../…../…. compatible effectiveness and adequacy of the controls established on information systems and we do not comment on its compatibility.

Editing Place and Date of the Report

Responsible Information Systems Lead Auditor

Name and Surname, Signature

Commercial Title of the Organization