(Reference) Reporting Leakage of Personal Information or Any Other Related Incident

I. Reporting Leakage of Personal Information or Any Other Related Incident

1. Members shall promptly report any leakage of personal information or any other related incident (including loss and damage of such information) (hereinafter referred to as "Leakage or Any Other Related Incident") to supervisory authorities, etc. and the Association. In this case, reporting to the Association shall be made using Form 1;

   provided, however, that incidents such as wrong transmission of fax, wrong delivery of postal mail or wrong transmission of e-mail may be collectively reported on about a quarterly basis to simplify the service procedures, if members decide, after screening each incident to identify the volume of leaked information, presence of sensitive information, and risk of secondary damage or occurrence of similar cases, that there is no substantial need to report the incidents immediately. In this case, reporting to the Association shall be made using Form 2.

2. When the details of an incident reported under 1. above has been identified, they shall be transferred to supervisory authorities and the Association without delay as "Update".

3. As a general rule, incidents which are not attributable to members, such as wrong delivery by a postal employee, shall not need to be reported; provided, however, that when it is uncertain that "no right or interest of the subject person is infringed, and the possibility that such infringement will take place in the future is inexistent or minimal", such incidents need to be reported immediately, at each occurrence or collectively on about a quarterly basis, after review of the circumstances described in the proviso to 1. above.

4. Members shall ensure the adequate internal management of Leakage or Any Other Related Incident described in 1. above, by keeping an internal record of the details, customer service, correction or improvement measures, etc. concerning the incidents.

II. Points of Attention When Making a Report (Form 1)

1. New/Update (of the last report dated)

   A report provided in I., 1. above shall be made and marked as "New", and a report set forth in I., 2. as "Update".

2. Department, etc. in which the incident occurred

Specify the department in which the Leakage or Any Other Related Incident occurred. Specify also the branch name if the incident occurred in a branch.

3. Department, title, etc. of the person responsible for the incident

Specify the department, title and other information of the person in charge who caused the Leakage or Any Other Related Incident, excluding information that allows identifying a specific individual such as name.

4. Date of occurrence

Write “Unknown” if the date of occurrence is unknown.

5. Date of discovery

Specify the date on which the Leakage or Any Other Related Incident was discovered.

6. Details of the information leaked, etc.

Specify the type, details and quantity of the information which leaked (including the quantity of sensitive information, if any). Specify also the breakdown by type of information (“personal data”, or “personal information and processing method, etc. related information”).

7. Information protection measures such as encryption

In the column “Information protection measures such as encryption”, specify whether any measures had been taken concerning the information before its leakage.

8. Party to which the information was leaked

Specify whether the party to which the information was leaked has been identified, the status of recovery of personal information, etc.

9. Circumstances of the incident

Select the item which describes how the Leakage or Any Other Related Incident occurred. Specify the details of the circumstances in parentheses as needed.

10. Details on the discovery of incident

Specify the date on which the incident was discovered and the event which led to that discovery (such as notice from the party to which the information was leaked, complaint from a customer, internal control, and reporting from the person in charge).

11. Status of notification to customers, etc.

About dealing with a customer, etc. (subject person) who suffered the Leakage or Any Other Related Incident, such as providing factual information, specify the department in charge, number of customers dealt with, status of dealing, etc.

12. Whether or not the incident was made public

If the incident is or was made public, specify the date of publication.

13. Details and method of publication

Specify the details and method of publication, and attach the documents made available to the public. If the incident was not made public, specify the reason.

14. Analysis of cause, recognition of issues, etc.

Specify how and why the Leakage or Any Other Related Incident occurred, as well as the status of compliance with internal rules, etc. on the security control over personal information and personal data.

15. Measures to prevent a recurrence, etc.

Specify any measures taken to prevent a recurrence.

16. Remarks

State other matters as reference, if any.

17. Reporting to supervisory authorities, etc.

Specify the status of reporting to supervisory authorities, etc.

(Note)

- The notification to the Association shall be made after excluding the information which will enable identification of a specific individual from the report.
- Form 2 shall be prepared following the fill-in instructions given at its bottom.

Form 1

Date:

To: Chairman of Japan Investment Advisers Association

Company name

Name of the Member's representative

Report on Leakage of Personal Information, etc.

Under the provisions of Article 22, paragraph (1) of the "Procedural Guidelines on the Protection of Personal Information" (Resolution of the Board of Directors on March 23, 2005), we hereby report as follows on a Leakage or Any Other Related Incident of Personal Information, etc. which occurred recently.

1. New/Update (of the last report dated)			
2. Department, etc. in which the incident occurred		3. Department, title, etc. of the person responsible for the incident	
4. Date of occurrence		5. Date of discovery	
6. Details of the information leaked, etc.			
7. Information protection measures such as encryption	□ Taken □ Partially taken □ Not taken □ Unknown		
8. Party to which the information was leaked			
9. Circumstances of the incident	□ Wrong transmission of fax □ Wrong transmission of e-mail □ Hand delivery to wrong person □ Delivery to wrong address □ Oral disclosure □ Disposal by error □ Loss □ Other ( ) 〔 〕		
10. Details on the discovery of incident			

Date:

11. Status of notification to customers, etc.			
12. Whether or not the incident was made public		(Date of publication)	
13. Details and method of publication (If the incident is not made public, specify the reason)			
14. Analysis of cause, recognition of issues, etc. (Specify also the status of compliance with internal rules, etc.)			
15. Measures to prevent a recurrence, etc.			
16. Remarks			
17. Reporting to supervisory authorities, etc.		□ Done □ Undone	

Principal contact Department and title:

Name: Phone no.:

Form 2.

Date:

To: Chairman of Japan Investment Advisers Association

Company name

Name of the Member's representative

Report on Leakage of Personal Information, etc.

Under the provisions of Article 22, paragraph (1) of the "Procedural Guidelines for the Protection of Personal Information" (Resolution of the Board of Directors on March 23, 2005), we hereby report as follows on a Leakage or Any Other Related Incident of Personal Information, etc. which occurred recently.

Department, etc. in which the incident occurred	Number of persons subject to the leakage	Type, details, etc. of the information					Date of occurrence, date of discovery	Source of leakage	Person responsible for the incident	Intentional or unintentional	Notification to customer	Overview of the case	Ex-post measures		Remarks	／ New/Update
		Type of information	Details of information	Sensitive information	Type of information (personal data, or personal information and processing method, etc. related information)	Information protection measures such as encryption							Measures to prevent a recurrence	Other measures		
Department: ____	___ persons	Information of a customer Information of an employee Other information	Name: Date of birth: Gender: Address: Other ( )	Contained Not contained	Personal data only Personal information and processing method, etc. related information (excluding personal data) only Both	Taken Partially taken Not taken Unknown	Date of occurrence: Date of discovery:	The Company Entrusted persons (deliverer) Entrusted persons (other:)	Employee of the Company Employee of entrusted persons Third party Other ( ) Unknown	Intentional Unintentional Unknown	Intentional Unintentional	Wrong transmission of fax Wrong transmission of e-mail Delivery to wrong address Other ( )	Technological security control measures Human security control measures Institutional security control measures Other ( )			/ New/ Last report Date:
Department: ____	___ persons	Information of a customer Information of an employee Other information	Name: Date of birth: Gender: Address: Other ( )	Contained Not contained	Personal data only Personal information and processing method, etc. related information (excluding personal data) only Both	Taken Partially taken Not taken Unknown	Date of occurrence: Date of discovery:	The Company Entrusted persons (deliverer) Entrusted persons (other:)	Employee of the Company Employee of entrusted persons Third party Other ( ) Unknown	Intentional Unintentional Unknown	Intentional Unintentional	Wrong transmission of fax Wrong transmission of e-mail Delivery to wrong address Other ( )	Technological security control measures Human security control measures Institutional security control measures Other ( )			/ New/ Last report Date:
Department: ____	___ persons	Information of a customer Information of an employee Other information	Name: Date of birth: Gender: Address: Other (Phone no.)	Contained Not contained	Personal data only Personal information and processing method, etc. related information (excluding personal data) only Both	Taken Partially taken Not taken Unknown	Date of occurrence: Date of discovery:	The Company Entrusted persons (deliverer) Entrusted persons (other:)	Employee of the Company Employee of entrusted persons Third party Other ( ) Unknown	Intentional Unintentional Unknown	Intentional Unintentional	Wrong transmission of fax Wrong transmission of e-mail Delivery to wrong address Other ( )	Technological security control measures Human security control measures Institutional security control measures Other ( )			/ New/ Last report Date:

Form 2.

Date:

Department, etc. in which the incident occurred	Number of persons subject to the leakage	Type, details, etc. of the information					Date of occurrence, date of discovery	Source of leakage	Person responsible for the incident	Intentional or unintentional	Notification to customer	Overview of the case	Ex-post measures		Remarks	／ New/Update
		Type of information	Details of information	Sensitive information	Type of information (personal data, or personal information and processing method, etc. related information)	Information protection measures such as encryption							Measures to prevent a recurrence	Other measures		
(Total)	___ persons	Information of a customer: __ case(s) Information of an employee: __ case(s) Other information: __ case(s)	Name: __ case(s) Date of birth: __ case(s) Gender: __ case(s) Address: __ case(s) Other: __ case(s)	Contained: __ case(s) Not contained: __ case(s)	Personal data only: __ case(s) Personal information and processing method, etc. related information (excluding personal data) only: __ case(s) Both: __ case(s)	Taken: __ case(s) Partially taken: __ case(s) Not taken: __ case(s) Unknown: __ case(s)		The Company: __ case(s) Entrusted persons (deliverer): __ case(s) Entrusted persons (other): __ case(s)	Employee of the Company: __ case(s) Employee of entrusted persons: __ case(s) Third party: __ case(s) Other: __ case(s) Unknown: __ case(s)	Intentional: __ case(s) Unintentional: __ case(s) Unknown: __ case(s)	Intentional: __ case(s) Unintentional: __ case(s)	Wrong transmission of fax: __ case(s) Wrong transmission of e-mail: __ case(s) Delivery to wrong address: __ case(s) Other: __ case(s)	Technological security control measures: __ case(s) Human security control measures: __ case(s) Institutional security control measures: __ case(s) Other: __ case(s)			

* Mark the corresponding item with "○".
* In the column "Department, etc. in which the incident occurred", add the name of branch to the name of department if the incident occurred in a branch.
* In the column "Department, etc. in which the incident occurred", specify only the entrusting department, etc. if the information was leaked to entrusted persons.
* Write "Unknown" if the date of occurrence is unknown.
* When more than one report is made on the same case, make sure that there is no multiple counting in "(Total)".
* In the column "Information protection measures such as encryption", specify whether any measures had been taken concerning the information before its leakage, etc.

Principal contact Department and title: Name: Phone no.