



The ID Register

Incident Response Plan

November 2019



The ID Register – Incident Response Plan

I. Policy Statement

The ID Register (“the ID Register”) Incident Response Plan (“IRP”) outlines ID Register’s recommended actions following a data incident in order to ensure that incidents affecting the ID Register’s computing systems and Personal Information maintained by the ID Register are handled in a consistent manner that minimizes the potential impact of those incidents on the ID Register’s clients, business and reputation.

II. Overview and Purpose

The ID Register has taken steps to reduce the risk of a data incident, many of which are outlined in the ID Register’s Written Information Security Program (“WISP”). However, no protection is foolproof and many data incidents occur as a result of human error. Therefore, the ID Register must be prepared to respond to a data incident in the event that one should occur. This IRP provides guidance for relevant personnel as to how they should respond in the event that a data incident occurs.

III. Scope

This IRP covers all the ID Register locations. It pertains to all the ID Register information technology systems, including, but not limited to, telephone, email, database, computer and networking systems and electronically stored information which contains Personal Information. This IRP also covers all paper records that contain Personal Information.

This IRP covers all the ID Register employees and other persons who maintain or access Personal Information, in paper or electronic form.

IV. Definitions

Computing Device – any device or medium upon which the ID Register data is stored in electronic form. Computing Devices may be either the ID Register-owned or personal devices and include, but are not limited to, computers, tables, smartphones, portable hard disks and USB storage devices.

Data incident - The unauthorised access to, acquisition or use of Personal Information that creates a risk of identity theft, fraud or harm to an individual.

A data incident can take many different forms. This IRP specifically addresses four categories of data incidents, however, **any situation in which an ID Register employee is concerned that there might be a potential threat to Personal Information should be treated as a potential data incident and reported to the ID Register management team by individual email or via the helpdesk (help@theidregister.com)**

- Unauthorised access to IT Systems
 - An unauthorised third party uses an exploit to gain access to the ID Register’s IT
 - An unauthorised party obtains legitimate access credentials to ID Register IT systems by means of social engineering.

- Breach of security of Personal Information
 - Unauthorised third party gains access to Personal Information
 - The ID Register employee misappropriates Personal Information
 - Third party is mistakenly given access to Personal Information (e.g., an email or document containing Personal Information is sent to the incorrect third party)

- Lost Computing Device
 - Computing Device containing Personal Information is lost or stolen.
- Ransomware
 - A type of malicious software designed to block access to a computer system until a sum of money is paid.

When a third party vendor reports a data incident to the ID Register that involves Personal Information controlled by the ID Register, the incident should be treated as a potential data incident.

ID Register – The ID Register, including the ID Register and, to the extent permitted by applicable local law, any of its affiliated companies to which it is associated by common ownership or control.

Personal Information as defined by the The Gramm-Leach-Bliley Act (GLB Act)

Personal Information - Personal Information means any information concerning an individual, including The ID Register employees and clients that, if improperly accessed or acquired, would create a risk of identity theft or fraud to the individual. For the purposes of this Program, Personal Information includes: (a) all non-public personal information as defined by the G-L-B Act and all applicable rules and regulations thereunder, including Regulation S-P and (b) “personal information” as it is defined under the Massachusetts Standards for the Protection of Personal Information of Residents of the Commonwealth.

Examples of personal information include, but are not limited to an individual’s first and last name or first initial and last name, in combination with:

- Social Security number;
- Driver’s license number or state-issued identification card number;
- Account number, credit card or debit card number, with or without any required security code, access code, personal identification number (PIN) or password, that would permit access to a person’s account;
- Information a consumer provides to the ID Register on an application to obtain a service from the ID Register;
- Account balance information, payment history, overdraft history, and credit or debit card purchase information; or
- The fact that an individual is or has been an ID Register customer or has obtained a service from ID Register.

Information that relates to institutional investors who are not individual natural persons is not “Personal Information.”

Personal Data as defined under article 4 of The General Data Protection Regulation

1. ‘Personal data’ means any information relating to an identified or identifiable natural person (‘data subject’); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person;

V. Roles and Responsibilities

- Employees are the ID Register’s first line of defence against data incidents and all ID Register employees and personnel are responsible for identifying and reporting potential data incidents. All potential data incidents should be reported to help@theidregister.com or to a member of the management team via email.

- The ID Register Director is responsible for evaluating all potential data incidents that are reported to help@theidregister.com or to a member of the management team and for identifying and evaluating all potential data incidents generally.
- The ID Register Director has primary responsibility for incident response and will oversee the investigation of the incident. The ID Register Director is also responsible for convening the Incident Response Team when needed, for coordinating communications amongst the members of the Incident Response Team and for taking reasonable steps to document all data incidents and the subsequent responsive actions taken in relation to them. If the Director determines that immediate action needs to be taken in order to stop a data incident and/or preserve forensic data relating to a data incident, the Director is authorised to take those actions as soon as he or she deems reasonably necessary (and prior to a meeting of the Incident Response Team) in order to mitigate further risk of harm.
- **The Incident Response Team consists of the ID Register Director and the ID Register Management Team consisting of the Legal Manager, the Project Manager and the Operations Manager.** The Incident Response Team is responsible for determining the appropriate actions to take in response to a data incident and deciding which additional parties (internal and external) will be involved in the data incident response depending on the nature of the data incident and type(s) of information involved.

VI. Response Plan

Initial Response – A Manager and the Director

Where the incident relates to internal factors, for example, an error made by a staff member, the manager of that individual will provide a summary of the incident to the management team and Director. Where the incident relates to external factors, the management team will nominate a manager to provide the initial summary.

In response to suspected data incidents, the relevant manager will:

1. Conduct a preliminary investigation: Gather details about the incident, including when the breach was first

discovered and any responsive actions taken.

2. Make an initial determination about whether Personal Information was involved in the data incident: Inquire about the nature of records or data involved in the breach and what kinds of information it contained.

- If it is suspected that the data incident did not involve Personal Information: The Manager will inform the Director. If the Director determines that no further action needs to be taken in response to the data incident, the Director or his or her designee will work with the Manager to prepare a short description of the data incident which will be saved to G:\Investor Services\Legal\Incidents
- If it is suspected that the data incident involved Personal Information: The Manager will contact the Director, who will then convene a meeting of the Incident Response Team. To the extent the Director determines that immediate action needs to be taken in relation to the data incident in order to stop the data incident or mitigate the potential negative consequences of the data incident prior to the time the Incident Response Team convenes, the Director is authorised to take such action.

3. Investigation and Recovery – The Director in conjunction with the Incident Response Team.

Given the varied nature of data incidents involving Personal Information, the Incident Response Team will respond to data incidents on a case-by-case basis. Some data incidents may be dealt with internally while others may require the Incident Response Team to reach out to third parties including, but not limited to, outside legal counsel, information security consultants, forensic experts and public relations teams.

Outlined below are guidelines for how the Incident Response Team should go about responding to four common types of data incidents. While the Incident Response Team will generally work together on incident response, the Director is primarily responsible for incident response.

A. Unauthorised Access to IT Systems

Upon learning of unauthorised access to the ID Register's IT systems, the Director should immediately be notified. The Director should specifically attempt to determine whether the unauthorised access threatens the security, confidentiality, or integrity of Personal Information. If it does, the procedures set forth under "Breach of Security of Personal Information" herein should be followed.

The Incident Response Team will engage the following parties as needed in any instance of potential unauthorized access to the ID Register's IT systems:

- Legal
 - Be actively involved with investigation.
 - Determine if a referral to law enforcement, civil litigation, or regulatory reporting is appropriate.
- Subject Matter Experts
 - Assess the business impact of the unauthorised access and advise Legal and/or the Incident Response Team regarding the severity level of the event.
- Human Resources
 - Determine if an ID Register employee is responsible or otherwise complicit in the unauthorised access.

B. Breach of Security of Personal Information

Both state and federal law (USA) impose significant obligations on businesses which experience a breach in security of Personal Information. In order to ensure that the ID Register responds to any such breach in a timely and compliant manner, it is imperative that all known or potential security breaches be thoroughly investigated. Because the ID Register's obligations following a security breach vary significantly depending on a number of factors, including the type of information subject to unauthorised disclosure, the physical location of the data subjects, and the number of individuals affected, the ID Register Legal and outside legal counsel (as needed) should be closely involved in the investigation from the outset.

Upon learning of a potential breach in the security of Personal Information, the breach should immediately be brought to the attention of the Director and the Incident Response Team, which should begin an investigation in order to:

1. Validate that a breach has actually occurred;
2. Ensure that the security breach is not ongoing;
3. Determine the nature of the Personal Information subject to unauthorised access, including:
4. What types of data may have been accessed (e.g., names, account numbers, social security

- numbers, addresses, etc.);
- A. Which and how many individuals' Personal Information may have been accessed;
- B. Whether any of the Personal Information in question was protected by encryption; and
- C. Whether the individuals whose Personal Information may have been accessed are
- D. employees or non-employees;
- E. Make an initial determination of the severity level of the breach;
- 5. Gather evidence of the security breach and take steps to preserve same;
- 6. Document the security breach, and
- 7. Determine what, if any, changes in the ID Register's IT security practices should be made to prevent a recurrence of the security breach.

The Incident Response Team will engage the following parties as needed when there is a potential data incident involving a breach of security of Personal Information:

- Legal (including outside legal counsel as needed)
 - Be actively involved with investigation into the circumstances of the security breach.
 - Determine whether the ID Register has any reporting obligations under applicable state or federal law.
 - If so, inform breach notification vendor.
 - Notify regulatory authorities if required under applicable law.
- Assess whether the security breach should be reported to law enforcement or regulatory authorities.
- Review communications to employees or clients prior to dissemination.
- Review and sign off on the Incident Report.
- Human Resources
 - Determine if breached Personal Information includes data relating to employees.
- Investor Relations and Corporate Communications
 - Prepare press statement relating to the security breach if needed.
 - To be reviewed by Legal prior to dissemination.

C. Lost Computing Device

Upon being informed of the loss or theft of an ID Register Computing Device the relevant Manager should immediately, to the extent possible, (1) determine what data was resident on the device at the time of its loss and whether that data was encrypted; and (2) take steps to remotely erase all data from the device.

- If the device contained Personal Information, the incident should be responded to in the manner described under "Breach of Security of Personal Information"

D. Ransomware

Ransomware is a type of malware that prevents a user from using a computer, network or other device until a certain amount of money is paid. Ransomware generally works by locking the interface of or encrypting the data on a computer, network or other device. Once the interface is locked or the data is encrypted, the user will not be able to access the interface or data without the encryption key. The criminals behind the ransomware hold the encryption key and demand payment (often through an anonymous payment system like Bitcoin) for its release, promising to provide the encryption key if the ransom is paid within a certain amount of time. However, even if the ransom is paid, there is no guarantee that the encryption key will be provided. In addition, even if the encryption key is provided, the downtime caused by the ransomware attack can cost the ID Register more than the actual ransom paid. Failing to pay the ransom means that the targeted data is permanently lost.

Upon learning of a potential data incident involving ransomware, the Operations Director will be

notified. The Incident Response Team will engage the following parties, as needed, when there is a potential data incident involving ransomware:

- IT staff (including external IT consultants as needed)
 - Determine whether and how to isolate the affected systems from the network and the Internet.
 - Determine what type of malware is being dealt with and how to remove the threat.
 - Work with Legal and the ID Register executives to determine whether, and how, the ID Register
 - Business Continuity Plan should be implemented.
 - Work with Legal and the ID Register executives to determine whether to pay the ransom, understanding that doing so may increase the likelihood that the ID Register may be directly targeted for additional extortion attempts in the future.
 - Determine how and when to restore any impacted data from a known backup.
- Legal (including outside legal counsel as needed)
 - Be actively involved with the investigation into the circumstances of ransomware.
 - Determine whether the ID Register has any reporting obligations under applicable state or federal law.
 - Assess whether the security breach should be reported to law enforcement authorities (local and/or federal).
 - Review and sign off on the Incident Report.

E. System Availability and Usage

Data Incidents as defined in this policy represent a risk to the security of personal information. The ID Register is, however, exposed to other Information Technology risks which also have the potential to disrupt employee and client use of the ID Register and this represents a separate risk to the business.

Where a user experiences an issue with The ID Register, this issue must be raised to the ID Register Business Analyst. The Business Analyst in conversation with the Project Manager will then determine if the impact is critical or minor in nature.

In the case of critical issues the Incident Response Team should be convened and hold an emergency meeting with Developers and Information Technology (including external IT consultants as needed)

- Determine and isolate the root cause of the issue
- Determine how and when to restore any impacted data from a known backup.

If such critical issues are identified in the testing period following a system enhancement, the ID Register Director must be notified immediately by the Business Analyst and manager on duty who will determine if it is appropriate to rollback the enhancement.

VII. Documenting a Data Incident

Reasonable steps should be taken to create a contemporaneous written record of all data incidents. An Incident Report should be prepared and should include a description of the incident, the identity of the individual who discovered it, a description of the incident response, details of any investigation, the final resolution of the incident and any remedial steps that were taken (including any necessary revisions to this IRP or the ID Register's WISP). The Director should indicate whether the data incident will need to be specifically reported to the Board of Trustees. Legal review and signoff on each Incident Report should be obtained.

VIII. Enforcement

Any employee who neglects to report a known security breach, or who fails to comply with this plan in any other respect, may be subject to disciplinary action, up to and including termination. In appropriate cases, the ID Register may refer violations of this IRP to law enforcement officials.

IX. Policies Cross-Referenced

Written Information Security Program

Business Continuity Plan

X. Effective Date

This Incident Response Plan is effective from 16 January 2017 and supersedes all prior policies. This policy has been updated on 25 April 2018.