Minnesota FAIR Plan

Data Breach Response Policy

Purpose

This policy establishes how the MN FAIR Plan will respond in the event a data breach, and also outlines an action plan that will be used to investigate potential breaches and to mitigate damage if a breach occurs. This policy is in place to both minimize potential damages that could result from a data breach and to ensure that parties affected by a data breach are properly informed of how to protect themselves.

Scope

This policy applies to all incidents where a breach of customer or employee personal identifying information is suspected or confirmed.

DEFINITIONS

Personal Identifying Information– information that can be used to distinguish or trace an individual's identity. Personal Identifying information includes, but is not limited to, any of the following:

- Social Security numbers
- Payment information (bank account information, credit card information, etc.)
- Tax identification information numbers (Social Security numbers; business identification numbers; employer identification numbers)
- Payroll information (paychecks; paystubs)
- Other personal information of a customer, employee or contractor (dates of birth; addresses; phone numbers; maiden names; names; customer numbers)

Breach – any situation where personal identifying information is accessed by someone other than an authorized user, for anything other than an authorized purpose.

POLICY GUIDELINES

Upon Learning of a Breach

A breach or a suspected breach of personal identifying information must be immediately investigated. Since all personal identifying information is of a highly confidential nature, only personnel necessary for the data breach investigation will be informed of the breach. The following information must be reported to appropriate management personnel:

- When (date and time) did the breach happen?

- How did the breach happen?
- What types of personal identifying information were obtained? (Detailed as possible: name; name and social security; Name, account and password; etc.)
- How many customers were affected?

Management will then make a record of events and people involved, as well as any discoveries made over the course of the investigation and determine whether or not a breach has occurred.

Perform a Risk Assessment

Once a breach has been verified and contained, perform a risk assessment that rates the:

- Sensitivity of the personal identifying information Lost (customer contact information alone may present much less of a threat than financial information)
- Amount of personal identifying information lost and number of individuals affected
- Likelihood personal identifying information Is usable or may cause harm
- Likelihood the personal identifying information was intentionally targeted (increases chance for fraudulent use)
- Strength and effectiveness of security technologies protecting personal identifying information (e.g. encrypted personal identifying information on a stolen laptop. Technically stolen personal identifying information but with a greatly decreased chance of access.)
- Ability of to mitigate the risk of harm

All information collected during the risk assessment must then be compiled into one report and analyzed. The risk assessment must then be provided to appropriate personnel in charge of data breach response management.

Notifying Affected Parties

Responsibility to notify is based both on the number of individuals affected and the nature of the personal identifying information that was accessed. Any information found in the initial risk assessment will be turned over to the legal counsel of who will review the situation to determine if, and to what extent, notification is required. Notification should occur in a manner that ensures the affected individuals will receive actual notice of the incident. Notification will be made in a timely manner, but not so soon so as to unnecessary compound the initial incident with incomplete facts or to make identity theft more likely through the notice.

In the case that notification must be made:

- Only those that are legally required to be notified will be informed of the breach. Notifying a broad base when it is not required could cause raise unnecessary concern in those who have not been affected.
- A physical copy will always be mailed to the affected parties no matter what other notification methods are used (e.g. phone or email).
- A help line will be established as a resource for those who have additional

questions about how the breach with affect them.

The notification letter will include:

- A brief description of the incident. The nature of the breach and the approximate date it occurred.
- A description of the type(s) of personal identifying information that were involved in the breach. (The general types of personal identifying information, not an individual's specific information.)
- Explanation of steps being taken to investigate the breach, mitigate its negative effects and prevent future incidences.
- Steps the individual can take to mitigate any potential side effects from the breach.
- Contact information for a representative who can answer additional questions.

Mitigating Risks

Based off the findings of the risk assessment, a plan will be developed to mitigate risk involved with the breach. The exact course of action will be based on the type of personal identifying information that was involved in the data breach. The course of action will aim to minimize the effect of the initial breach and to prevent similar breaches from taking place.

- Affected individuals will be notified as soon as possible so they can take their own steps to mitigate potential risk.
- If there is a substantial concern for fraudulent use of personal identifying information, MN FAIR Plan will offer affected individuals free access to a credit monitoring service.
- MN FAIR Plan will also provide steps to mitigate risks that can be taken by affected individuals. The steps provided to affected individuals will depend on the nature of the data breach. If the breach has created a high risk for fraudulent use of financial information, customers may be advised to:
    - Monitor their financial accounts and immediately report any suspicious or fraudulent activity.
    - Contact the three major credit bureaus and place an initial fraud alert on their credit reports. This can be extremely helpful in situations where personal identifying information that can be used to open new accounts, such as social security numbers, has been taken.
    - Avoid attempts from criminals that may see the breach as an opportunity to pose as employees in an attempt to deceive affected individuals into divulging personal information.
    - File a report with local police or in the community where the breach took place.
    - Complete a Federal Trade Commission Threat Affidavit, available at www.ftc.gov/bcp/edu/resources/forms/affidavit.pdf. This form will allow the affected individual to notify their creditors that their identity has been compromised, and will minimize their liability for fraudulent use of their identity.
- MN FAIR Plan will also include instructions on what steps a customer can take to reduce their risk will be included in the notification letter. In addition to the information listed above, appropriate personnel, when possible, will provide additional information tailored to the individual breach.