

CONSUMER INFORMATION PROTECTION GUIDANCE

DIVISION OF BANKING AND FINANCIAL INSTITUTIONS

June 15, 2007

The Gramm-Leach-Bliley Act (GLBA) is the federal law that requires financial institutions to ensure the security and confidentiality of customer personal information. The Federal Trade Commission (FTC) has determined financial institutions include payday lenders, title lenders, finance companies, mortgage lenders, mortgage brokers, and non-depository lenders. The State of Montana, Division of Banking and Financial Institutions (Division) is the agency that licenses and regulates these businesses.

In accordance with GLBA and state law, the following information is to be provided to customers that may have had their information compromised:

Customer notice* should be given in a clear and conspicuous manner. The notice should describe the incident in general terms, and the type of customer information that was the subject of loss, unauthorized access, or use. It also should generally describe what the licensee has done to protect the customer's information from further unauthorized access. In addition, the notice should include a telephone number that customers can call for further information and assistance. The notice also should remind customers of the need to remain vigilant over the next 12 to 24 months, and to promptly report incidents of suspected identity theft to the licensee, local law enforcement, the Montana Attorney General's Office of Consumer Protection, and the Federal Trade Commission. The notice should include the following additional items, when appropriate:

1. A recommendation that the customer review account statements and immediately report any suspicious activity to the licensee;
2. A description of fraud alerts and an explanation of how the customer may place a fraud alert in the customer's consumer reports to put the customer's creditors on notice that the customer may be a victim of fraud;
3. A recommendation that the customer periodically obtain credit reports from each nationwide credit reporting agency, and have information relating to fraudulent transactions deleted;
4. An explanation of how the customer may obtain a credit report free of charge; and
5. Information about the availability of the Montana Attorney General's Office of Consumer Protection and the FTC's online guidance regarding steps a consumer can take to protect against identity theft. The notice should encourage the customer to report any incidents of identity theft to the Office of Consumer Protection and FTC, and should provide these agencies' website addresses and toll-free telephone numbers that customers may use to obtain the identity theft guidance and report suspected incidents of identity theft.

Customers should be notified within 10 business days. Customer notice should be delivered in a manner designed to ensure that a customer can reasonably be expected to receive it.

*If a licensee, based upon its investigation, can determine from its logs or other data, precisely which customers' information has been improperly accessed, it may limit notification to those customers with regard to whom the licensee determines that misuse of their information has occurred or is reasonably possible. However, there may be situations where the licensee determines that a group of files has been accessed improperly, but is unable to identify which specific customers' information has been accessed. If the circumstances of the unauthorized access lead the licensee to determine that misuse of the information is reasonably possible, it should notify all customers in the group.

Licensees are expected to provide the following information to the Division by telephone and mail as soon as possible after the discovery of loss or suspected loss:

1. Report private personal information has been compromised.
2. Provide a copy of the information that has been compromised, if it is available.
3. Identify and report reasonably foreseeable internal and external threats to confidential information.
4. Assess and report the likelihood and potential damage to customers.
5. Detail the sufficiency of policies and procedures to control these risks.
6. Describe the incident in sufficient detail.

The Division expects licensees to implement a Personal Information Loss/Embezzlement Response to address incidents of lost, stolen, or unauthorized access of confidential customer and examination information. The plan must encompass all licensee operations. The program will specify actions to be taken when any licensee suspects or detects that nonpublic personal customer information has been compromised. This policy is to be communicated to all locations to ensure each branch and employee understands the procedures that must be followed when information is lost or evidence suggests that information has been compromised.

All licensees are required to:

1. Develop an information security program that assesses risks to confidential, nonpublic customer information.
2. Evaluate and modify practices, policies, and procedures to minimize the unauthorized disclosure, misuse, alteration, or destruction of customer information. The licensee should:
 - Limit access to customer information or customer information systems to authorized individuals. Controls should be designed to prevent employees from providing information to unauthorized individuals.
 - Perform background checks on employees with responsibilities that include accessing customer information.
3. Institute response programs that specify actions to be taken when the licensee suspects or detects unauthorized individuals have gained access to customer information systems, including alerting appropriate regulatory and law enforcement agencies. The response program should include:
 - Identification of what customer information systems and types of customer information have been breached.
 - Notification to the Division as soon as possible.
 - Notification to appropriate law enforcement authorities.
 - Notation of appropriate steps to be taken to contain and control the incident to prevent further unauthorized access or use of information.
 - Notification to customers when warranted.

If you have questions regarding this guidance, please contact the Division at 406/841-2920.

Division of Banking and Financial Institutions Theft Reporting Form

Reporting Date: _____

Licensee & License #: _____

Address: _____

Amount of Theft: \$ _____

Date of Incident: _____

Discovery Date: _____

Date law enforcement notified: _____

Contact name: _____

Contact phone number: _____

Suspect (If known. Otherwise state "Unknown")

Name: _____

Address: _____

ID Type: _____

Number: _____

Description of Theft:

- _____ Embezzlement
- _____ Robbery
- _____ Fraud
- _____ Identity Theft
- _____ Break-in
- _____ Other (describe) _____

Reported by: _____
(print name & title)