



## University of Minnesota Identity Theft Prevention Program

### Self-Identification Questionnaire

The University of Minnesota must comply with a three-part federal regulation known as “The Red Flags Rule”. The University of Minnesota’s *Identity Theft Prevention Program* describes our compliance requirements under the law.

The *Identity Theft Prevention Program* has three sections, each with distinct compliance requirements.

- The main section describes the four “red flags” elements representing the bulk of the Program.
- A special requirements section relates to the use of consumer reporting agencies.
- A third section describes the special duties of card issuers.

Use this quick guide as a first-step to determine if your area is in-scope and thus must comply with this regulation. Specific compliance requirements are described in the *Identity Theft Prevention Program* and in the RFR Compliance Guidance document available on the [Controller's Office website](#).

1. Does any unit in your area use consumer reports or provide information to consumer reporting agencies? Examples might be in relation to background checks in certain areas of hiring or admission, or credit checks as part of certain loan activities.

*If yes, those units must comply with the special requirements relating to the use of consumer reporting agencies.*

2. Does any unit in your area issue a credit or debit card? Stored value cards such as the U Card (Gopher Gold) and payroll deduct cards (but not gift cards) are considered debit cards in this legislation.

*If yes, those units must comply with the special duties of card issuers.*

3. Does any unit in your area offer or maintain credit or deposit accounts that allow multiple payments or transactions? Examples include federal and institutional loans, and certain types of tuition payment plans.

*If yes, those units must comply design, implement and maintain processes to detect, respond and mitigate identity theft in connection with covered accounts.*

4. Does any unit in your area offer or maintain a credit or deposit account for which there is a reasonably foreseeable risk to customers or the University of identity theft?

*If yes, those units must comply design, implement and maintain processes to detect, respond and mitigate identity theft in connection with covered account.*

Contact the Controller's Office with questions at <mailto:finsys@umn.edu>, or 612-624-1617. Guidance and training materials available at: <http://www.finsys.umn.edu/controller/redflags.html>.