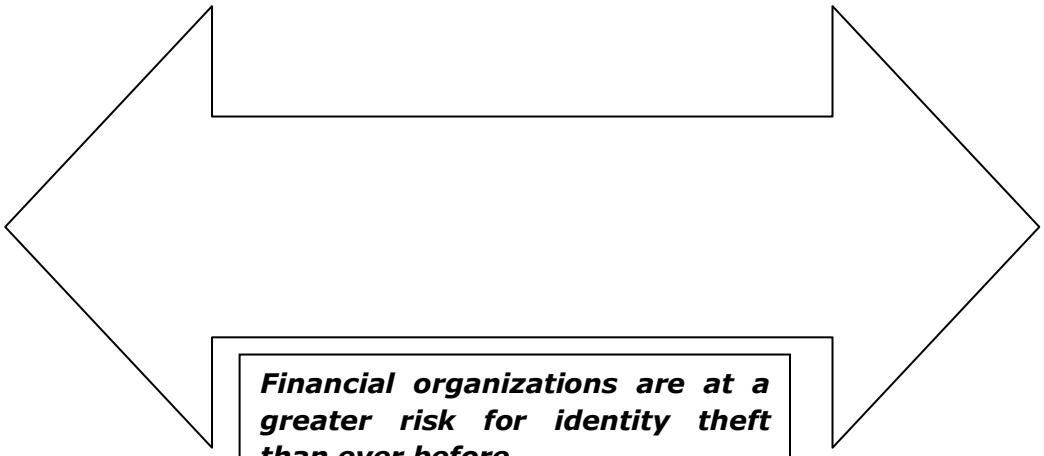
Oversight of Service Provider Arrangements

Whenever a financial institution or creditor engages a service provider to perform an activity in connection with one or more covered accounts the financial institution or creditor should take steps to ensure that the activity of the service provider is conducted in accordance with reasonable policies and procedures designed to detect, prevent, and mitigate the risk of identity theft.

For example, a financial institution or creditor could require the service provider by contract to have policies and procedures to detect relevant Red Flags that may arise in the performance of the service provider's activities, and either report the Red Flags to the financial institution or creditor, or to take appropriate steps to prevent or mitigate identity theft.



Financial organizations are at a greater risk for identity theft than ever before.

The document that follows covers any organization that has access to your customers nonpublic personal information (NPI) or personal identifiable information (PII) such as banks, telemarketing, direct mail, cleaning services or other third party vendors that would or could have access to these records be responsible for either or both safeguards and Identity Theft prevention.

Sierra Credit Corp – (Third Party Vendor Name)

Dear Sir or Madam:

We require that all companies, with whom we transact business to confirm to us in writing that any and all personal health information (PHI) received from us through our relationship will be kept, stored and maintained in accordance with the law. Additionally, we require all companies to confirm to us in writing that they are compliant with FACT Act Red Flags Rules and have in place an Identity Theft Prevention Program (ITPP)

CONFIDENTIAL CUSTOMER INFORMATION

We agree to regard and preserve, as confidential, all information obtained by or disclosed to us by or at your direction about your customers, including but not limited to name, address, telephone number, account number, policy information and any list or grouping of customers ("Customer Information"), and to use such information solely in the manner contemplated and authorized by our business relationship.

We agree not to disclose and not to permit our employees to disclose Customer Information for any purpose other than in furtherance of our business relationship. Upon termination of our business relationship, or any time you request, we shall promptly return to you, or destroy all Customer Information in our possession except for our business records.

We further agree to implement and maintain an effective information security program to protect your Customer Information.

The program shall include administrative, technical and physical safeguards to: a) ensure the security and confidentiality of Customer Information; b) protect against any anticipated threats or hazards to the security or integrity of such Customer Information; and c) protect against unauthorized access to or use of Customer Information which could result in substantial harm or inconvenience to you or your customers.

If we are not in compliance with the requirements regarding Customer Information, we shall immediately tell you and take steps to correct the non-compliance, including but not limited to protecting customers and you against the consequences of any disclosure or use of Customer Information in violation of this Agreement.

Section VI(c) of the guidelines provides that, whenever a financial institution or creditor engages a service provider to perform an activity in connection with one or more covered accounts, the financial institution or creditor should take steps to ensure that the activity of the service provider is conducted in accordance with reasonable policies and procedures designed to detect, prevent, and mitigate the risk of identity theft.

Thus, the guidelines make clear that a service provider that provides services to multiple financial institutions and creditors may do so in accordance with its own program to prevent identity theft, as long as the program meets the requirements of the regulations. The guidelines also provide an example of how a covered entity may comply with this provision. The guidelines state that a financial institution or creditor could require the service provider, by contract, to have policies and procedures to detect relevant Red Flags that may arise in the performance of the service provider's activities and either report the Red Flags to the financial institution or creditor or take appropriate steps to prevent or mitigate identity theft.

We agree that that we shall comply with all identity theft red flag and notice of address discrepancy laws, rules and regulations now and in the future to protect customer's identity information. We agree to implement (if we have not already done so) and maintain appropriate processes and procedures as required by FACT Act Red Flags Identity Theft Prevention Program.

SAFEGUARDING CUSTOMER NONPUBLIC PERSONAL INFORMATION (NPI)

_____ _____
PRINT NAME DATE

_____ _____
SIGNED TITLE

FACT ACT RED FLAGS IDENTITY THEFT PREVENTION PROGRAM

_____ _____
PRINT NAME DATE

_____ _____
SIGNED TITLE

FACT Act Identity Theft Prevention Program