MOORE NORMAN TECHNOLOGY CENTER

POLICY # **323**

Adopted: December 18, 2014

BOARD OF EDUCATION POLICY

IDENTITY THEFT PREVENTION

This policy is adopted to ensure compliance with the Fair and Accurate Credit Transaction Act, 15 USC. §1601 et seq. and the Federal Trade Commission's rule regarding Identity Theft (the "Red Flag Rules"). The technology center is subject to the Red Flag rules if it is a "Creditor." The technology center is a Creditor if it provides any goods or services for a fee and as a matter of course extends credit to its customers by offering them the ability to pay for those goods and services after they are provided as opposed to requiring prepayment or contemporaneous payment. The technology center is a creditor with respect to limited areas involving a low risk of identity theft. Areas in which the technology center allows a debtor to defer payment owed the technology center include, but are not limited to, adult education tuition, facility use charges and similar accounts. The technology center must review all of its "Accounts" to determine whether any of those accounts are "Covered Accounts." As to "Covered Accounts," it must develop an Identity Theft Program (herein referred to as the "Program") designed to detect, prevent, and mitigate identity theft in connection with a Covered Account.

Definitions

For purposes of this policy, the following definitions apply.

"Account" means a continuing relationship established by a person with the technology center to obtain a product or service for personal, family, household, or business purposes. Note that the requirements of the federal rules apply not only to existing accounts but also to new account openings, when a relationship has not yet been established.

"Technology center" means Moore Norman Technology Center.

"Covered Account" pertains to accounts which involve prepayment or contemporaneous payment as well as payment in arrears and means (i) an account that the technology center offers or maintains, primarily for personal, family or household purposes, that involves or is designed to permit multiple payments or transactions, such as a tuition account, or facility rental account and similar accounts; and (ii) any other account that the technology center offers or maintains for which there is a reasonably foreseeable risk to customers or to the safety and soundness of the technology center from identify theft, including financial, operational, compliance, reputation, or litigation risks. This category of Accounts includes the technology center's small business accounts, sole proprietorship accounts, and accounts for which the risk of identity theft is reasonably foreseeable because of how they are opened and accessed (i.e., the accounts can be accessed without face-to-face contact, such as through the Internet or by telephone).

"Credit" means the right granted by the technology center to a debtor to defer payment of debt or to incur debts and defer its payment or to purchase property or services and defer payment therefore.

"Creditor" means a business or organization that regularly defers payment for goods or services or provides goods or services and bills customers later (as opposed to requiring prepayment or contemporaneous payment).

"Customer" means a person that has a covered account with the technology center.

"Identity Theft" means fraud committed or attempted using identifying information of another person without authority. "Person" means a natural person, a corporation, government or governmental subdivision or agency, trust, estate, partnership, cooperative, or association.

"Personal Identifying Information" means a person's credit card account information, debit card information, bank, bank account information, and driver's license information and for a natural person includes the individual's social security number, mother's birth name, and date of birth.

"Red Flag" means a pattern, practice, or specific activity that indicates the possible existence of identity theft.

"Service Provider" means a person that provides a service directly to the technology center.

<u>Creation of Identity Theft Program</u>

1. The technology center shall create an Identity Theft Program to protect Covered Accounts. At a minimum, the Program will:

2. Identify and list the Covered Accounts
3. Identity and list the red flags indicating that someone might be attempting to obtain services, products or information surreptitiously by claiming to be someone they are not.
4. Explain how the technology center will detect red flags that been identified.
5. Explain how the technology center will respond if a red flag is detected.
6. The Director of Finance will administer the program.
7. Describe the technology center staff who need to be trained on how to detect and respond to identity theft and the training they should receive.
8. To ensure the protection of the technology center clients from identity theft via the technology center contracted service providers, identity the categories of service providers that should be required via contract to assist the technology center in detecting red flags and must therefore either have their own red flags program or ensure compliance with the technology center's red flag program.
9. Be submitted to the technology center's board for approval.
10. Be annually re-evaluated to determine whether material changes have occurred warranting changes to the technology center's identity theft policy and programs

Updating the Program

Upon the recommendation of the superintendent, the board of education shall annually review and, as deemed necessary by the board, update the technology center's identity theft prevention program along with any relevant red flags in order to reflect changes in risks to customers or to the safety and soundness of the technology center and its covered accounts from identity theft. In so doing, the board shall consider the following factors and exercise its discretion in amending the program:

1. The technology center's experience with identity theft;
2. Updates and methods of identity theft;
3. Updates and customary methods used to detect, prevent, and mitigate identity theft;
4. Updates on the types of accounts that the technology center offers or maintains; and
5. Updates in service provider arrangements.

Reference: 15 U.S.C 1061 et seq.