# Table of Contents

<table>
<thead>
<tr>
<th>Section</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Introduction</strong></td>
<td></td>
</tr>
<tr>
<td>Government Identity Theft Initiatives Overview</td>
<td>2</td>
</tr>
<tr>
<td>Impact on the Mortgage Industry</td>
<td>2</td>
</tr>
<tr>
<td>Liability for Non-Compliance</td>
<td>3</td>
</tr>
<tr>
<td>Our Commitment to Creating a Responsible Work Environment</td>
<td>3</td>
</tr>
<tr>
<td><strong>Red Flag Policy</strong></td>
<td></td>
</tr>
<tr>
<td>Red Flag Policy Overview</td>
<td>4</td>
</tr>
<tr>
<td>What is Non-Public Personal Information</td>
<td>4</td>
</tr>
<tr>
<td>Types of Identity Theft</td>
<td>5</td>
</tr>
<tr>
<td>Types of Identity Theft “Red Flags” to be Aware of</td>
<td>5</td>
</tr>
<tr>
<td>Obtaining NPI and Verifying Customer Identities</td>
<td>5</td>
</tr>
<tr>
<td>NPI Risk from Employees</td>
<td>6</td>
</tr>
<tr>
<td>Activities that Pose Risk Which are External to Company Offices</td>
<td>7</td>
</tr>
<tr>
<td>Activities that Pose Risk Which are Internal to Company Offices</td>
<td>8-9</td>
</tr>
<tr>
<td>Red Flags – Quick Reference List</td>
<td>10-11</td>
</tr>
<tr>
<td><strong>Red Flag Rules &amp; Safeguards</strong></td>
<td></td>
</tr>
<tr>
<td>Red Flag Rules and Procedures</td>
<td>12-13</td>
</tr>
<tr>
<td>Identifying and Assessing Risk to NPI</td>
<td>14</td>
</tr>
<tr>
<td>Securing the Personal Information of our Borrower at our Work Stations</td>
<td>15</td>
</tr>
<tr>
<td>Shred Boxes in Work Stations</td>
<td>16</td>
</tr>
<tr>
<td>Electronic Information Systems</td>
<td>16</td>
</tr>
<tr>
<td>Data Protection and Management</td>
<td>17</td>
</tr>
<tr>
<td>Hard Copy Files and Documents</td>
<td>17</td>
</tr>
<tr>
<td>Disposal of NPI Documents and Electronic Storage Devices</td>
<td>18</td>
</tr>
<tr>
<td>Safeguards</td>
<td>18</td>
</tr>
<tr>
<td><strong>Service Providers</strong></td>
<td></td>
</tr>
<tr>
<td>Selection and Oversight of Service Providers</td>
<td>19</td>
</tr>
<tr>
<td><strong>Information Security Officer</strong></td>
<td></td>
</tr>
<tr>
<td>Appointment &amp; Responsibilities of the Information Security Officer</td>
<td>20-21</td>
</tr>
<tr>
<td>How to Report Violations</td>
<td>21</td>
</tr>
<tr>
<td>Training</td>
<td>21</td>
</tr>
<tr>
<td><strong>Exhibits</strong></td>
<td></td>
</tr>
<tr>
<td>Information Security Program Endorsement</td>
<td>22</td>
</tr>
<tr>
<td>Appointment of the Information Security Officer</td>
<td>23</td>
</tr>
<tr>
<td>Employee Acknowledgement – ISP Requirements &amp; Employee Responsibilities</td>
<td>24</td>
</tr>
</tbody>
</table>
Government Identity Theft Initiatives Overview

In October 1998, the U.S. Congress enacted the Identity Theft and Assumption Deterrence Act, (the ITAD Act), which made identity theft a federal crime and charged the Federal Trade Commission (FTC) with taking complaints from identity theft victims, sharing their complaints with federal, state and local law enforcement, and providing the victims with information to help them restore their good name.

The FTC was instructed to log and acknowledge complaints of individuals who believed they were victims of identity theft and to report such complaints to the three credit repositories as well as the appropriate law enforcement agency for potential law enforcement action.

With the passage of the Gramm Leach Bliley Act (the GLB Act) in 1999, and the Fair and Accurate Credit Transactions Act (FACTA) in 2003, the Federal Trade Commission was given power to prosecute organizations for contributing to the identity theft problem by the careless handling of sensitive personal information.

These two new laws specifically included all components of the mortgage industry as “covered entities” under the Acts and provided specific instruction as to how to comply with the law and set forth penalties for non-compliance. While most of the industries that are included under “covered entities,” have made concerted efforts to comply with these laws, many mortgage companies have gone uninformed and are now being subjected to fines and penalties by the FTC for non-compliance.

Impact on the Mortgage Industry

The government continues to pass additional legislation as a means to deter those individuals and organizations that collect, handle and store “at risk” personal information for legitimate business purposes. All entities are required to be sensitive to their personal responsibilities as custodians of such information.

It is for this very reason that mortgage companies are finding themselves the focus of increased scrutiny by the FTC.

The Federal Trade Commission has issued regulations requiring financial institutions and creditors to develop and implement written identity theft prevention programs, as part of FACTA. These programs must be in place by November 1, 2009 and must provide for the identification, detection and response to patterns or specific activities – known as “red flags” – that could indicate identity theft.
Liability for Non-Compliance

FACTA disposal rules apply to any business that directly or indirectly has or uses “consumer information,” regardless of the size of the business or the number of employees. Every business is mandated to keep its records safe and dispose of them properly. FACTA provides for a range of civil liabilities and penalties for non-compliance.

A business that fails to comply with FACTA rules can be liable for actual damages in a civil lawsuit brought on by anyone whose identity is stolen as a result. FACTA also allows class action lawsuits to be filed, a state fine of $1,000 per willful or negligent violation and federal fines of up to $2,500 per infraction.

The Gramm Leach Bliley Act (GLB Act) gives authority to eight federal agencies and states to administer and enforce the Financial Privacy Rule and the Safeguards Rule. Civil and criminal penalties under the Safeguards Rule include fines of up to $100,000 for each violation and criminal penalties may include up to five years in prison.

The Identity Theft Enforcement and Protection Act of 2005 (ITEP Act) mandates that businesses have a legal duty to protect and safeguard sensitive personal information. Similar to the GLB Act, the ITEP Act requires business to implement and maintain procedures and corrective measures to protect the consumer. Furthermore, the ITEP Act includes a “Dumpster Diving” provision requiring companies to destroy customer records that are no longer in use by shredding, erasing or modifying the records to make the information undecipherable or unreadable. The ITEP Act also allows the Attorney General to seek a permanent injunction and exposes defendants to a civil penalty of at least $2,000 per violation, up to a maximum of $50,000.

In addition, the Deceptive Trade Practices-Consumer Protection Act (DTPA) can impose a civil penalty against each defendant up to $20,000 for each violation.

The repercussion, due to the mishandling of NPI is a serious offense – as evidenced in each Act above. Mistakes are costly to all involved and sensitive care is required at all times by all Ark-La-Tex Financial Services, LLC employees who handle NPI. Every employee is required to adhere to the parameters set forth by Ark-La-Tex Financial Services, LLC in a conscientious effort to comply with the Information Security Plan put in place for our organization.

Our Commitment to Creating a Responsible Work Environment

Ark-La-Tex Financial Services, LLC is committed to creating a responsible work environment with the implementation of an Information Security Plan. Thirty to fifty percent (30-50%) of all identity theft originates on the workplace. Ninety (90%) of this is the result of carelessness and to a lesser extent, dishonest employees.

A mortgage loan file contains almost all of the personal and credit information a customer possesses. Due to the nature of the processing, underwriting, closing, funding, shipping and other functions – almost everyone will have access to the loan file. The proper understanding, attitude and enforcement towards the security of the Non-Public Personal Information (NPI) must be understood and adhered to by all Ark-La-Tex Financial Services, LLC employees.

Employees who violate the Information Security Plan will be terminated.
Identity Theft Red Flags Detection & Prevention Guidelines

Red Flag Policy Overview

The security and protection of our customer’s and employee’s Non-Public Personal Information (referred to herein as NPI) is a top priority in our organization. Of each employee, we expect the greatest sensitivity in the handling of documents and data containing NPI. Each of us has a responsibility to our customers and each other to be alert to who has access to work areas and data devices where NPI is accessed and/or stored. Any actions or events observed by an employee that raise suspicion of a possible security breach of NPI must be reported to the Information Security Officer or their designate and the event will be aggressively investigated and analyzed for validity. If a security breach has occurred, a mitigation program will be implemented immediately.

As used in these policies and procedures and relating to customers and employees, NPI will be defined as any personal identifying items or information held by this company.

Ark-La-Tex Financial Services, LLC requires that all employees take the utmost care when handling a borrower’s personal information. Every employee is responsible for ensuring that all borrower related information is put away from any possible public contact and/or viewing when not in use. The potential access or viewing of a borrower’s personal information by anyone who is not an approved Ark-La-Tex Financial Services, LLC employee is not permitted.

What is Non-Public Personal Information

The purpose of an Information Security Program is the prevention, detection and mitigation of identity theft risk associated with the handling and storage of Nonpublic Personal Information (NPI) belonging to our customers and employees. NPI is information in written, print or data form, to include but not limited to:

- Name
- Home Address
- Previous Address
- Phone Numbers
- Email Addresses
- Date of Birth
- Social Security Number
- Driver’s License Number
- Current or previous Employer Information
- Current or past income levels
- Tax records
- Banking or Creditor information – including account numbers
- Copies of Drivers License or Social Security Card
- Credit Card information
- Personal Check information

This information is most commonly found on loan applications, credit reports, pay-stubs, verification of employment forms, tax returns, bank statements, fax confirmations and photocopies obtained or provided by the applicant.
Types of Identity Theft
When a criminal steals another’s identity, it usually referred to in one of two forms. They are:

- **Assumption** – it refers to the total and complete assumption of another’s identity with the documentation to prove identity, most commonly of someone who is deceased or infirm
- **Cloning** – it refers to the criminals acquisition of another’s personal identifiers who then impersonates that person for the purpose of concealment of the criminals identity

These practices are commonly used to conceal a current or previous criminal history or a previous credit history. A common form of identity fraud experienced in the mortgage industry is when a loan applicant uses a cloned or assumed identity to secure a mortgage loan.

Types of Identity Theft “Red Flags” to be Aware of
There are two types of identity theft “red flags” that all employees must be aware of and knowledgeable about in their daily activities:

- The activity by an employee who mishandles an applicants NPI, which poses a risk and could result in the applicant having their identity stolen
- The taking/acceptance of a loan application by an applicant who is impersonating another whose identity may have or has been stolen

Obtaining NPI and Verifying Customer Identities
The following procedures will be implemented with respect to obtaining NPI and verifying customer identities:

- In order to accept an application for a mortgage loan, the Company must have a signed URLA, FNMA Form 1003, complete with applicant(s) names, addresses, telephone numbers, birth dates, social security numbers, and driver’s license (or other from of government issued photo identification), to enable the Company to verify the identification of the customers
- It is the responsibility of the loan originator to verify the loan applicant’s identity and will require a driver’s license or other form of government-issued photo identification to verify the applicant’s identity and will make a copy of the same to retain in the loan file
- Employees are required to match the loan applicant with the photo likeness found on the driver’s license
- If a face to face interview or meeting between the loan originator and a loan applicant is not possible, for whatever reason, the title company or closing agent will be instructed to make a reasonable attempt to verify the identity of the loan applicant and report back to the Information Security Officer or designate if the identity cannot be verified

In the event that NPI provided in documentation is conflicting or cannot be verified upon further inquiry, the employee shall request additional government-issued documentation evidencing the customer’s residence and bearing a photograph (i.e. alien identification card, or passport) to enable the employee to form a reasonable belief that they know a customer’s true identity. Employees will notify the Information Security Officer or a designate if a customer’s identity still cannot be verified.

In the event that NPI provided in documentation is conflicting or cannot be verified upon further inquiry, the employee shall request additional government-issued documentation evidencing the customer’s residence and bearing a photograph (i.e. alien identification card, or passport) to enable the employee to form a reasonable belief that they know a customer’s true identity. Employees will notify the Information Security Officer or a designate if a customer’s identity still cannot be verified.

In the event that NPI provided in documentation is conflicting or cannot be verified upon further inquiry, the employee shall request additional government-issued documentation evidencing the customer’s residence and bearing a photograph (i.e. alien identification card, or passport) to enable the employee to form a reasonable belief that they know a customer’s true identity. Employees will notify the Information Security Officer or a designate if a customer’s identity still cannot be verified.

In the event that NPI provided in documentation is conflicting or cannot be verified upon further inquiry, the employee shall request additional government-issued documentation evidencing the customer’s residence and bearing a photograph (i.e. alien identification card, or passport) to enable the employee to form a reasonable belief that they know a customer’s true identity. Employees will notify the Information Security Officer or a designate if a customer’s identity still cannot be verified.

In the event that NPI provided in documentation is conflicting or cannot be verified upon further inquiry, the employee shall request additional government-issued documentation evidencing the customer’s residence and bearing a photograph (i.e. alien identification card, or passport) to enable the employee to form a reasonable belief that they know a customer’s true identity. Employees will notify the Information Security Officer or a designate if a customer’s identity still cannot be verified.
NPI Risk from Employees

The most frequent access to NPI is by the people who are authorized to handle it and are charged with the responsibility of securing this sensitive material. It is the organizations responsibility to see that the people who join the company and will be authorized to handle NPI are honest and of good character.

NPI documents and data are at risk when authorized individuals engage in one of the following activities:

<table>
<thead>
<tr>
<th>Activities</th>
<th>Safeguards</th>
<th>Red Flags</th>
</tr>
</thead>
<tbody>
<tr>
<td>• Looses or misplaces an NPI document</td>
<td>• Adopt strong hiring policies to include reference, character background and credit report checks to make sure there are not previous acts of neglect or malfeasants</td>
<td>• Employee makes statements about having difficulty meeting credit obligations</td>
</tr>
<tr>
<td>• Is careless and knowingly violates the company’s Information Security Policies and Procedures</td>
<td>• Maintain close contact with each employee to detect if there is an incentive or reason to compromise NPI for monetary gain</td>
<td>• Employee asks for an untimely raise</td>
</tr>
<tr>
<td>• Knowingly allows an unauthorized individual to obtain or have access to the NPI document</td>
<td>• Maintain a high awareness in the company environment to follow ISP Policies and Procedures</td>
<td>• Follow up credit report shows an employee to have over extended credit items</td>
</tr>
<tr>
<td>• Takes the NPI to use or sell for personal gain</td>
<td>• Maintain a high awareness with each employee of the disciplinarian actions for not following ISP Policies and Procedures</td>
<td>• An employee behaving in a strange, nervous or defensive manner</td>
</tr>
<tr>
<td>• Is the victim of an act of God and the NPI document is lost</td>
<td></td>
<td>• An employee expresses concern over a fellow employee’s family, credit, or monetary issues</td>
</tr>
</tbody>
</table>

It is common and usual for an individual having domestic issues to share their problems with others. Although it is time for compassion, it is also time to assess the risk these problems could pose to NPI. It is possible for people of good character to compromise their otherwise solid principals to protect themselves or their family (and therefore warrants further investigation).
Activities that Pose Risk to NPI Which are External to Company Offices

There are a number of activities conducted outside the office that are necessary to the operation of a mortgage origination organization. These activities are considered to pose a greater risk to NPI than activities conducted in the office where the environment is more closely monitored.

These activities include:

<table>
<thead>
<tr>
<th>Activities</th>
<th>Safeguards</th>
<th>Red Flags</th>
</tr>
</thead>
<tbody>
<tr>
<td>✷ Accepting a loan application from an individual who may be assuming the identity of another person</td>
<td>✷ It is the responsibility of the loan originator to verify the loan applicant's identity and will require a driver’s license or other form of government-issued photo identification to do so – make a copy to retain in the loan file</td>
<td>✷ Inability to fully verify an applicants identity</td>
</tr>
<tr>
<td>✷ Face to face loan application interviews in the field which could be either hand written applications or data entry on laptops</td>
<td>✷ The laptop or written 1003 is to remain with the originator at all times – at no time is it permissible to leave NPI in an unsecure location</td>
<td>✷ Missing or stolen laptop computer, or other data storage devise</td>
</tr>
<tr>
<td>✷ Collection of supporting documents in the field such as pay stubs, W-2’s, bank statements, creditors and account numbers, identification documents, personal checks, etc.</td>
<td>✷ All NPI collected from the applicant must remain with the originator at all times in a secure manner, such as a locked briefcase – at no time is it permissible to leave NPI out in the open of a vehicle</td>
<td>✷ Lost or missing loan documents</td>
</tr>
<tr>
<td>✷ Accessing, downloading and printing credit reports in the field</td>
<td>✷ Credit reports should be printed in Adobe and uploaded to MDB in the e-Briefcase or into DocumentTrac in WebTrac</td>
<td>✷ Unauthorized and persons unrelated to the transaction overseeing the completion of a loan application or data entry of a loan application</td>
</tr>
<tr>
<td>✷ Employees conducting processing functions of loan applications at home</td>
<td>✷ Great care must be given to the secure handling of a borrower’s NPI at all times – the information must be kept in a secure location when not in use</td>
<td>✷ Any unauthorized person making or offering to make copies of documents containing NPI</td>
</tr>
<tr>
<td>✷ Disposal of documents in the field</td>
<td>✷ All printed material containing NPI must be immediately shredded or placed in a secure disposal bin for future shredding by a service provider</td>
<td>✷ NPI left out in the open for viewing by an unauthorized party</td>
</tr>
</tbody>
</table>
Activities that Pose Risk to NPI Which are Internal to Company Offices

There are a number of activities conducted inside the office that are necessary to the operation of a mortgage origination organization. These activities could pose a risk to NPI unless closely monitored.

These activities include:

<table>
<thead>
<tr>
<th>Activities</th>
<th>Safeguards</th>
<th>Red Flags</th>
</tr>
</thead>
<tbody>
<tr>
<td>• Accepting a loan application for an applicant who may be assuming the identity of another person</td>
<td>• Positively verify the identity of each applicant and obtain a copy of the identification card</td>
<td>• Inability to fully verify an applicants identity</td>
</tr>
<tr>
<td>• Discovering inconsistencies during loan review such as names, signatures, dates, addresses, etc.</td>
<td>• Document inconsistencies are found during loan review</td>
<td>• Inability to clarify inconsistencies found during loan review</td>
</tr>
<tr>
<td>• Written loan application, supporting documents or client's personal check dropped off at the receptionist desk</td>
<td>• All visitors are required to sign in before entering a secure office area and also must signing out when leaving</td>
<td>• Unfamiliar persons in secure work areas</td>
</tr>
<tr>
<td>• Written loan application, supporting documents or client's personal check received by mail in the company office</td>
<td>• Incoming loan documents received by mail, courier or dropped at the company’s office will be delivered to the LO or processor or record unopened</td>
<td>• Familiar but unauthorized persons lingering in secure work areas</td>
</tr>
<tr>
<td>• Supporting documents prepared by third party service providers delivered by mail, courier or dropped at receptionist desk</td>
<td>• Incoming loan documents received by mail, courier or dropped at the company’s office will be delivered to the appropriate department immediately</td>
<td>• Unauthorized persons viewing data entry or processing of loan documents</td>
</tr>
<tr>
<td>• Loan files open in a work area visible to unauthorized persons</td>
<td>• Loan documents received at the receptionist desk will be maintained in a secure drawer or file cabinet until retrieved by appropriate department</td>
<td>• Inquiries by previous clients or unknown persons about information being extracted on the company’s behalf such as an inquiry on a credit report that was not initiated by the company</td>
</tr>
<tr>
<td>• Printing NPI to a shared printer in a common area; printed information remains in tray or on work table</td>
<td>• Immediately rise and retrieve any NPI documentation from a shared printer</td>
<td>• Credit reports received with Fraud Alerts, Activity Duty Alerts, or a Credit Freeze</td>
</tr>
<tr>
<td>• Transporting loan files between departments</td>
<td>• All users must lock keyboard or log out of websites/applications that contain NPI of our applicants</td>
<td>• Notification by a service provider of a security breach involving company’s clients or employees</td>
</tr>
<tr>
<td>• Scanning or faxing documents to third party service providers</td>
<td>• Remain with fax package if it contains any NPI documentation</td>
<td>• Notification by a law enforcement agency of a security breach involving company’s clients or employees</td>
</tr>
</tbody>
</table>
### Continued:

<table>
<thead>
<tr>
<th>Activities</th>
<th>Safeguards</th>
<th>Red Flags</th>
</tr>
</thead>
<tbody>
<tr>
<td>✷ Receiving faxed documents</td>
<td>• Immediately rise and retrieve any NPI documentation from a shared fax machine or printer where the information may have been printed</td>
<td></td>
</tr>
<tr>
<td>✷ Sending fax documents</td>
<td>• Retrieve the items received via faxed from the fax tray if they contain NPI documentation</td>
<td></td>
</tr>
<tr>
<td>✷ Properly storing loan documents and files when not in use</td>
<td>• Retrieve the fax confirmation from the confirmation tray as many times the confirmation will reflect the 4th page of the faxed package and this page will contain NPI for a borrower</td>
<td></td>
</tr>
<tr>
<td>✷ Careless practices of sharing logon information to company and services provider systems</td>
<td>• Do not share logins or passwords – direct inquiring individual to the Help Desk to obtain own login</td>
<td></td>
</tr>
<tr>
<td>✷ Computer or server hacking of company and service providers by unauthorized persons for the purpose of stealing client and employee NPI</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
Red Flags – Quick Reference List

The purpose of the list below is not to make you doubtful of every loan that crosses your desk, but rather make you aware of items in loan packages that should signal caution – a red flag. While a red flag does not constitute proof that a file contains misrepresented, it can alert you to potential problems.

<table>
<thead>
<tr>
<th>Loan Applications</th>
<th>Credit Reports</th>
<th>Verifications of Income</th>
</tr>
</thead>
<tbody>
<tr>
<td>Invalid SSN</td>
<td>Recent inquiries from mortgage lenders</td>
<td>Employee name or company is not printed on checks</td>
</tr>
<tr>
<td>Unsigned/Undated 1003</td>
<td>Social security numbers do not match</td>
<td>Handwritten checks</td>
</tr>
<tr>
<td>Significant changes in income from initial 1003 to final 1003</td>
<td>Credit report indicates “aka” or “dba”</td>
<td>SSN does not match 1003</td>
</tr>
<tr>
<td>Property size inadequate in relation to number of occupants</td>
<td>Credit bureau cannot verify borrower’s employment</td>
<td>W-2 is types but paystub is computer generated</td>
</tr>
<tr>
<td>Borrower’s age and number of years employed are not consistent</td>
<td>All accounts recently paid in full (possible debt consolidation loan undisclosed)</td>
<td>W-2 is not “Employee’s Copy” (Copy C)</td>
</tr>
<tr>
<td>Same phone number for business and home</td>
<td>Credit report debt is inconsistent with what is reflected on 1003</td>
<td>W-2 is inconsistent with 1003, paystubs and tax returns</td>
</tr>
<tr>
<td>Accumulation of assets inconsistent with income level</td>
<td>Credit report dated prior to 1003</td>
<td>Even dollar amount in YTD earnings</td>
</tr>
<tr>
<td>Years of school not congruent with profession</td>
<td>Length of established credit is inconsistent with applicant age</td>
<td>Verbal VOE is to voicemail or residence</td>
</tr>
<tr>
<td>Income not consistent with type of employment</td>
<td>High income borrower with low “high credit” limits</td>
<td>Date of hire on weekend or holiday</td>
</tr>
<tr>
<td>“other” employment not consistent with primary employment</td>
<td>Employment, residence or personal data does not match other sources in file</td>
<td>Numbers that appear “squeezed”</td>
</tr>
<tr>
<td>Borrower buying investment property but does not own current residence</td>
<td>All accounts were recently opened</td>
<td>Employer and applicants signature is the same</td>
</tr>
<tr>
<td>Type and use of credit is inconsistent with employment and income</td>
<td>Multiple SSN’s or names</td>
<td>Evidence of white out, strikeovers or alterations</td>
</tr>
<tr>
<td>P.O. Box is only indicated address for employer</td>
<td>Credit use or lack of use is inconsistent with income</td>
<td>Original VOE is not creased – indicates it was not mailed</td>
</tr>
<tr>
<td>Tax Returns</td>
<td>Verifications of Assets</td>
<td>Appraisals</td>
</tr>
<tr>
<td>------------------------------------------------</td>
<td>-------------------------------------------------------------------</td>
<td>-----------------------------------------------------------</td>
</tr>
<tr>
<td>Personal information does not agree with loan file</td>
<td>Even dollar amounts</td>
<td>Occupant is shown as tenant or unknown</td>
</tr>
<tr>
<td>High-income borrower with no deductions</td>
<td>Significant change over prior 2 months</td>
<td>“for rent” sign appears in photographs</td>
</tr>
<tr>
<td>Even dollar amounts for income or deductions</td>
<td>Recently opened account</td>
<td>Photos taken at odd angles</td>
</tr>
<tr>
<td>Self employed (SCH SE) does not reflect estimated tax payments</td>
<td>Deposits are inconsistent with reported income</td>
<td>Sales contract is dated after appraisal</td>
</tr>
<tr>
<td>W-2 does not match figures reported on 1040</td>
<td>Assets not consistent with income level</td>
<td>Property transferred within past 12 months</td>
</tr>
<tr>
<td>Paid tax preparer does not disclose TIN</td>
<td>Insufficient funds fees reported</td>
<td>House number in photos does not match appraisal and 1003</td>
</tr>
<tr>
<td>Paid tax preparer signed taxpayer copy</td>
<td>Account not in name of borrower or other names are associated with it</td>
<td>Comps are not verified as recorded</td>
</tr>
<tr>
<td>Handwritten returns prepared by professional tax preparer</td>
<td>Closing check is drawn on a different bank</td>
<td>Photos do not match description or reflects items not noted in the appraisal</td>
</tr>
<tr>
<td>Real estate owned but no deductions taken for taxes or interest paid (SCH A)</td>
<td>Account was opened on weekend or holiday</td>
<td>Comps all adjusted in the same direction</td>
</tr>
<tr>
<td>Stock owned but no dividend income reported (SCH B)</td>
<td>No date stamp affixed to document by depository</td>
<td>Comps more than 1 mile from subject property</td>
</tr>
<tr>
<td>Gross income does not agree with 1099 (SCH C)</td>
<td>Gift donor is not related or typical source</td>
<td>Line adjustments are in excess of 10%</td>
</tr>
<tr>
<td>Interest expense but no related loan is disclosed (SCH C)</td>
<td></td>
<td>Overall adjustments exceed 25%</td>
</tr>
<tr>
<td>No salary expense to operate business (SCH C)</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Properties listed but not disclosed on 1003 (SCH E)</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Mortgage interest deduction taken, but debt not disclosed on 1003 (SCH E)</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
Identity Theft Red Flags Detection & Prevention Guidelines

Red Flag Rules and Procedures
In order to comply with the Red Flag Rules as defined by FACTA of 2003 and outlined by the Federal Trade Commission which requires the detection, prevention, and mitigation of identity theft by loan applicants, the following warning signs or Red Flags shall be reported to the Information Security Officer.

For a mortgage origination company, Red Flags can be classified into two categories (1) Identity Validation Red Flags and (2) Event Red Flags. An Identity Validation Red Flag occurs when a loan applicant or employment applicant appears to be assuming another's identity using fraudulent documentation. An Event Red Flag occurs when there is an event that raises suspicion that NIP may be or already has been stolen.

An “Identity Validation Red Flag” shall exist when one of the following is identified by an employee:

- If an applicant cannot provide at least two (2) forms of identification and at least one (1) form of government photo identification
- If there are inconsistencies in the names on the photo ID and the other identification documents
- If the likeness of the applicant and that in the photo identification is questionable
- If the age, date of birth or physical descriptions on any identification document is inconsistent with the other identification documents or with the physical likeness of the applicant
- If the signature on any identification documents are inconsistent with that on the application documents
- If a “fraud alert” or “credit freeze” has been placed on the applicants credit report
- If a notice of “address discrepancy” is provided by a credit reporting agency
- If a representative of the company never has a face to face interview with the loan applicant
- If the name on the credit card, bank check, or other method of payment that identifies the owner is not consistent with the name on the identification documents

If an employee identifies a Red Flag, it will be reported immediately to the Information Security Officer along with any other pertinent documents. If the Information Security Officer determines the Red Flag likely represents an attempted or possible identity theft the Information Security Officer will take action to authenticate the identity of the person in question. Such actions may include but are not limited to:

- Complete a Drivers License Search
- Conduct a Address History Verification
- Conduct a Phone Number Verification
- Complete a Social Security Number Validation

If the Information Security Officer cannot authenticate the identity of the person in question, the “Managing System Failures and Mitigation Program” identified below will be implemented.
An “Event Red Flag” shall exist when one of the following is identified by an employee:

- If the loan applicant sends someone in his/her place to courier the loan application or closing documents to and from a remote site for signature
- If the loan applicant provides an “application supporting document” that does not appear to be authentic
- If a company employee request an exception to standard application or loan processing procedure
- If any employee or third party provider reports a security breach of data or information
- If an employee reports a missing, lost or stolen loan file or loan document containing an applicants NPI
- If any employee reports a missing, lost or stolen data storage devise such as a lap top containing applicants or employee NPI
- If the company receives an inquiry for loan status for a loan application that is not in the current “application log of applications received or in processing”
- If the company receives an inquiry from an unknown person about why a credit report or investigative report was ordered by the company
- If any employee witnesses or is party to any activity by an applicant or any person whose actions raise suspension of possible identity theft
Identifying and Assessing Risk to NPI

The risk to NPI can be divided into two categories (1) the storage of NIP documents and data and (2) the handling of physical NIP documents outside of storage by authorized persons. The safeguards and red flags for storage are far less than for the activities of authorized persons. When in storage NPI is considered beyond the control of the company.

Included in Policies and Procedures are requirements for the secure nature of physical file storage. Policies for insertion and extraction of physical and data files are covered in the assessment of risk in the handling of NPI documents and data. The responsibility for data security is placed on the software vendors and service providers who control the storage and transmission of data. The Policies and Procedures spell out the safeguards for NPI data by contract terms and warranty content of service providers to assure proper security of NPI data when in their domain. Therefore the risk assessment to follow does not include the details of storage and transmission of NPI data by vendors and service providers other than to briefly identify expectations for common preventative measures.

In the process of originating residential mortgage loans, risks to NPI documents and data exist from activities carried out in the office (a controlled environment) and in the field (an uncontrolled environment). The following risk assessment is divided into those in the field and those in the office. The focus of this assessment is on risk posed by:

- Employees and unauthorized persons seeking to capture NPI by covert means
- The careless practices of employees which could result in lost NPI
- Storage devises that protect NPI documents and data when not in use
- Loan applicants that assume the identity of another person

This assessment provides a basis for establishing safeguard policies to prevent identity theft and red flags to detect when identity theft may have occurred.
Securing the Personal Information of our Borrower at our Work Stations

Ark-La-Tex Financial Services, LLC requires that all employees take the utmost care when handling a borrower’s personal information. Every employee is responsible for ensuring that all borrower related information is put away from any possible public contact and/or viewing when not in use. The potential access or viewing of a borrower’s personal information by anyone who is not an approved Benchmark employee is not permitted.

If you leave your desk area, all employees must lock their system by selecting the “Windows logo” key and the letter “L” at the same time.

If you do not lock your keyboard, you must close/log off of all applications that contain sensitive borrower information [e.g., MDB, DO, Credco and DataTrac/WebTrac, etc].

Do not assume that because you are in an office that a borrower’s information cannot be accessed and breached – lock it up or log off.
Shred Boxes in Work Stations

All NPI items that are printed and necessitate shredding are to be placed in a secure bin for shredding each day – placing items in an open box in a common work area to be later delivered (days or weeks) to a shred bin is expressly prohibited and in violation of the Information Security Program.

At no time is it permissible to have the NPI of any borrower in an unsecure location. Before leaving for the day, all NPI (e.g. lead folders, lists, reports, files in process, fax confirmations, etc.) must be stowed in a secure cabinet or placed in a locked shred bin if applicable.

All offices must have an on-site shredder or locked shred bin awaiting disposal by a shredding service to handle the acceptable disposal of NPI.

Electronic Information Systems

The following information security standards will be implemented in order to protect electronic NPI collected and maintained by our Company.

- Employees will have access only to electronic NPI which is necessary to complete their designated responsibilities.
- Loan Officers and Loan Processors access to loan files on the LOS will be limited to those files originated by them or assigned to them.
- When using the loan application email capability of the LOS which is encrypted and password protected, passwords are not to be included in the body of the email.
- Access to electronic NPI will be password controlled. Every employee with access to the Company’s computer systems and electronic records will have a unique password consisting of at least eight (8) characters, including numbers and letters. Only employees that have a need to access electronic NPI records will be provided with such complex passwords.
- All company computers containing NPI or access to NPI will be equipped with password-activated screen savers to lock employee computers after a period of inactivity (not greater than 15 minutes).
- Employees shall log off of all Internet, E-mail and software applications when leaving their assigned work space or if their computer is not in use.
- Employees shall not post passwords in any insecure location or share passwords with any other person.
- Employees are not permitted to download any software, applications or data to or from Company computers.
- Employees are not to open e-mail attachments from unknown sources.
- Laptop or desk top computers containing NPI or access to NPI, whether company owned or employee owned, are to be kept in a secure area at all times and require complex password protection as previously described. All computers including employee owned laptops must have company approved firewalls, anti-virus software/spyware, and any other safeguarding software as may be dictated by the company from time to time. All such data protecting software is to be updated in accordance with providers recommendations.
- Any missing, lost or stolen laptop containing clients NPI must be reported to the Information Security Officer immediately.
Data Protection and Management
The following network data and management security standards will be implemented in order to protect
electronic NPI collected and maintained by our Company.

Network servers and web servers will be equipped with “Intrusive Prevention and Detection
System” software and will be monitored on a regular basis and updated as new versions are
made available by the vendor

All electronic NPI records will be stored on a secure server that is located in a locked room
and is accessible only by authorized persons

Backups of the computers and/or servers will be made at least once each day, or at more
frequent intervals as deemed necessary

All data will be erased from computers, disks, hard drives or any other electronic storage
devises that contain NPI before disposing of them and, where appropriate, hard drives will be
removed and physically destroyed

Hard Copy Files and Documents
The following hard copy files and documents security standards will be implemented in order to protect
electronic NPI collected and maintained by our Company.

Visitors, customers, vendors or service providers are not allowed unescorted in areas where
computers with access to client's NPI is kept

Because there are a substantial number of documents containing NPI that are received by
mail or fax, (1) no Company incoming mail will be opened by anyone other than the
addressee or a supervisor and (2) all incoming facsimile documents will be received on a
designated fax machine located in a secure area

Loan applicants will be directed to mail or deliver loan supporting documents only to one of
the company’s designated mailing addresses

Applicants who mail, courier, or drop loan documents for processing will be instructed to
place all documents in a sealed envelope, identifying to whose attention it is to be delivered

All files and documents will be stored in secure areas to which only authorized employees
will have access. All application loan documents must be stored in a fastener equipped loan
folder with all documents securely fastened

Application loan files and documents must be stored in a locked desk drawer or file cabinet
when unattended. Where appropriate, files and documents will be stored in a secure file
cabinet and/or at an offsite location

When transporting or taking loan applications in the field, loan files should be kept out of
sight and secured in a locked devise such as a briefcase

Employees are not permitted to remove, any files or documents containing customer or
employee NPI, from the Company premises
Disposal of NPI Documents and Electronic Storage Devices

All documents or electronic storage devices containing customer NPI will be destroyed in a manner consistent with the recommended guidelines of the Federal Trade Commission.

- It is in strict violation of company policy to dispose of loan documents or any document containing NPI in a trash can of any sort at any time.
- When loan documents are no longer required by regulation to be held by the company said documents are to be shredded in a confetti shredder. The company may equip the office with an acceptable shredder or have a shredding service collect loan documents form one or more on site central secure disposal container.
- Any electronic storage devise containing NPI will be first erased and then shredded by one of two means identified above.

Safeguards

All current employees and new hires, as well as independent contractors, who perform services on behalf of Ark-La-Tex Financial Services, LLC, will be subject to a satisfactory review of:

- Character reference checks
- Investigative background checks
- Consumer credit report
- Drug test

Each employee is required to participate in certain company activities to insure the security of NPI information and data; these activities shall include:

- Participation in the Company’s Information Security Program training program
- Sign and acknowledge an agreement to comply with the Company’s Information Security Program’s Policies and Procedures
- Protect the confidentiality and security of all NPI the Company collects on employees and clients
- Disclose to third party service providers only that NPI which has been authorized by the Information Security Officer
- Refer all unauthorized requests for NPI to the Information Security Officer
- Notify the Information Security Officer of any acts or attempts, by unauthorized persons, to obtain access to NPI and/or if any password or NPI is subject to unauthorized access.
- Only have access to employee or customer NPI if they have a business reason for seeing it
- Employees are not permitted to disclose the Information Security Program to any person without authorization from the Information Security Officer

Any employee that fails to abide by these Policies and Procedures of this Information Security Program, whether such failure is intentional or unintentional, will be subject to appropriate disciplinary action, which may include termination of employment.

When employment is terminated, the employee will attend an exit interview and return any keys in his/her possession that provide access to the Company’s offices, file cabinets, desks, etc. Passwords and security codes, if applicable, will be deleted; and employees will not be permitted to exit the premises with any Company property or material of any form.
## Selection and Oversight of Service Providers

In order to protect customer or employee NPI the Company collects, we will take steps to evaluate and oversee our service providers. The following evaluation criteria will be utilized in selecting service providers:

- Compatibility and willingness to comply with the Company’s Information Security Program and the adequacy of the service provider’s own Information Security Program
- Records containing NPI to be maintained by the service provider and the service provider’s methods for protecting such records are subject to reviewed at any time
- The service provider’s knowledge of regulations that is relevant to the services being provided, including privacy and other consumer protection regulations. Experience and ability to provide the necessary services and supporting technology for current and anticipated needs
- The adequacy of any service, systems and/or policies concerning the maintenance of secure systems, intrusion detection and reporting systems, customer authentication, verification, and authorization, and ability to respond to service disruptions. Service and support that will be provided in terms of maintenance, security, and other service levels
- Financial stability of the service provider and reputation with industry groups, trade associations and other companies
- Contractual obligations and requirements, such as the term of the contract; prices; software support and maintenance; training of employees; customer service; rights to modify existing services performed under the contract; warranty, confidentiality, indemnification, limitation of liability and exit clauses; guidelines for adding new or different services and for contract renegotiation; compliance with applicable regulatory requirements; records to be maintained by the service provider; notification of material changes to services, systems, controls and new service locations; insurance coverage to be maintained by the service provider; and use of the Company’s data, equipment, and system and application software
- All Service Providers will execute a “Service Provider’s Warranty and Indemnification” document as provided by the Company or a similar document or agreement provided by the Service Provider which contains at a minimum the terms of the Company’s document
- The right of the Company to audit any and all service provider’s records, (excluding intellectual property) to obtain documentation regarding the resolution of disclosed deficiencies, and to inspect the service provider’s facilities

Service Providers will be required to agree contractually to be responsible for securing and maintaining the confidentiality of NPI, including agreement to refrain from using or disclosing the Company’s information, except as necessary to or consistent with providing the contracted services, to protect against unauthorized use or disclosure of customer and Company information, to comply with applicable privacy regulations, and to fully disclose breaches in security resulting in unauthorized access to information that may materially affect the Company or its customers and to notify the Company of the services provider’s corrective action. Service providers will be subject to ongoing assessment to evaluate their consistency with selection criteria, performance and financial conditions, and contract compliance.
Appointment and Responsibilities of the Information Security Officer

Bryan Harlan will be the Information Security Officer for Ark-La-Tex Financial Services, LLC’s Information Security Program. In the event Bryan Harlan is unavailable, his designate will respond to inquiries and assist with the immediate resolve of any issues.

Specific duties and responsibilities for the Information Security Officer include:

- To identify and assess the risks to Non-public Personal Information retained by the Company on employees and customers and evaluate the effectiveness of current safeguards that have been implemented to mitigate those risks
- Create and implement the appropriate Information Security Program polices and procedures for Ark-La-Tex Financial Services, LLC regarding the sensitivity of the NPI we collect, handle, store and ultimately dispose of
- Regularly monitor and test the Information Security Program
- Designate and require the appropriate department to maintain a record of all locked drawers and file cabinets by inventory number, all persons who have access permission to each and all persons who have been issued a key to each – also to retain, for security purposes, a key to each locked drawer, work area, office and outside doors
- Designate and require the appropriate department to maintain an inventory of all computers and servers with list of who has access to each, be the lead administrator for and the custodian of all company software, providing adequate, secure storage for same, and maintain a record of where each software application has been installed
- Designate and require the appropriate department to maintain a record of all software, designated users, and on which computers or servers such software has been installed
- Designate and require the appropriate department to maintain a record of all service provider web interfaces, the users having access to such interfaces and the logon for each user
- Designate and require the appropriate department to verify each service provider’s web interface is equipped with acceptable encryption and authentication methods
- Assist with the selection of appropriate service providers that are capable of maintaining safeguards to protect the relevant NPI and reviewing service provider contracts to ensure that each contract contains the appropriate obligations with respect to the use of NPI and the implementation of safeguards
- Evaluate and adjust the Company’s Information Security Program in light of relevant circumstances, including changes to the Company’s operations, business relationships, technological developments and/or other matters that may impact the security or integrity of the Company’s NPI
- At the end of each day the Information Security Officer or designate will ensure that:
  - All desk drawers, file cabinets and offices are secure and/or locked
  - All copiers, fax machines, and scanners are empty
  - The LOS is backed up according to policy
- To report any violations of our Information Security Program, email compliance@benchmark.us
Pursuant to the USA Patriot Act and the Rules adopted by the Financial Crimes Enforcement Network (FinCEN), a Bureau under the Department of Treasury, the Information Security Officer will also be the contact person for Law Enforcement Agencies to provide the names of suspected terrorists and money launders in an effort to locate and secure loans involving those suspects. Upon receiving a request for information from FinCEN, the Information Security Officer will:

- Provide FinCEN with his/her name, title, and appropriate contact information, such as a mailing address, email address, telephone number and facsimile number, and notify FinCEN promptly of any modifications with respect to contact information.
- Ensure that information maintained by the Company, any loan applications received by the Company during the past 12 months, and any loans closed in the past, that the Company is required by law or regulation to keep, are searched to identify any names provided by FinCEN.
- If the Company has entered into a transaction with an individual or entity on the list, send a Report to FinCEN that contains: (1) The name of the individual, entity or organization; (2) The date and type of each loan transaction; and (3) The social security number, taxpayer identification number, passport number, date of birth, address, or other personal identifying information provided by the individual or entity at the time of the transaction.

Questions about the scope or terms of a request will be directed to the Law Enforcement Agency that sent the request for information to FinCEN, but the Report will be sent to FinCEN, not the Law Enforcement Agency that requested the search, unless the Information Security Officer is instructed otherwise.

**How to Report Violations**

To report any violations of our Information Security Program, email compliance@benchmark.us. Your report will be reviewed to resolve the issue.

**Training**

A training session is also available by selecting the following link:

Identity Theft Red Flags Detection & Prevention Overview
This Information Security Program has been reviewed by Bryan Harlan, Stewart Hunter and Jim McMahan of Ark-La-Tex Financial Services, LLC and is endorsed in its entirety and is hereby commissioned to be implemented and distributed to all employees both current and future.

As CEO of this Company, I want all to know that we place a high priority on and greatly value our customers and employees Nonpublic Personal Information "NPI" and will employ whatever methods, policies and practices to protect this information. I expect each employee of the Company and all with whom we hold contracts for operations related services, to acknowledge and hold to the standards outlined and addressed in this document.

Sincerely,

Bryan Harlan, CEO
26 October 2009

Ark-La-Tex Financial Services, LLC
5160 Tennyson Parkway, Suite 2000 W
Plano, Texas  75026

As part of Ark-La-Tex Financial Services, LLC’s comprehensive information security program, I am pleased to announcement that I will assume the designation as the Information Security Officer.  As Security Officer I will be responsible for designing, implementing and monitoring a security program to protect the security, confidentiality and integrity of personal information collected from and about our employees, consumers and vendors.

As Security Officer I will help the Company (1) identify material internal and external risks to the security of personal information, (2) design and implement reasonable safeguards and Red Flags to control the risks identified in the risk assessment, (3) evaluate and adjust the program in light of testing results, and (4) continuously monitor the program and procedures.

Thank you for your commitment to our company.

Sincerely,

Bryan Harlan, CEO
Employee Acknowledgement
Information Security Program Requirements & Employee Responsibilities

Date: ____________________________  
Branch Number: ____________________________  
Branch Manager: ____________________________  
Branch Address: ____________________________  
City / State / Zip: ____________________________

I acknowledge that I have read this handbook and understand the following:

Ark-La-Tex Financial Services, LLC is implementing an Information Security Program which will protect, detect and mitigate identity theft in the workplace

(Initial)

Among the highest priorities of Ark-La-Tex Financial Services, LLC is the protection of this information and I will adopt what ever measures necessary to achieve this objective

(Initial)

I understand adherence to these policies and procedures is a requirement of my employment with Ark-La-Tex Financial Services, LLC and do hereby agree to practice and enforce these Policies and Procedures

(Initial)

I further agree to notify the Information Security Officer or his designate immediately upon witnessing of or hearing of any breach of the Policies and Procedures

(Initial)

I understand that violating any provisions of these Policies and Procedures are subject to disciplinary actions which could result in my termination

(Initial)

I also understand the meaning of the term Nonpublic Personal Information (NPI) and that any actions on my part which results in customer or employee Nonpublic Personal Information falling into the hands of unauthorized individuals may be reported to the applicable law enforcement agencies and that if any criminal intent is involved, our Information Security Officer I will work closely with the law enforcement agencies to prosecute my actions which could result in civil and criminal penalties

(Initial)

Complete and email back to compliance@benchmark.us

Employee Signature ____________________________  Date ________________

Printed Name of Employee ____________________________

~ End of Guide ~