Table of Contents

Introduction

Our objective in is information security plan is to identify areas of risk within our operation, understand our obligations under the law, and to have formal procedures for resolving issues that arise with respect to sensitive consumer information. The Fair and Accurate Credit Transactions Act requires all financial service firms, including mortgage companies and mortgage brokers, to have an information security plan as well as a "Red Flag" program to identify whether consumers may already be victims of identity theft.

The new regulations provide financial institutions and creditors with flexibility in developing internal programs according to their relative organizational size and complexity. However, the Program must include reasonable policies and procedures that:

- identify relevant Red Flags, and then incorporate those Red Flags into the Program;
- detect such Red Flags;
- respond appropriately to any Red Flags to prevent and mitigate identity theft; and
- ensure that the Program is updated periodically to reflect changes in risks to customers

A red flag program is useless without an information security plan. At Company Name, the information security plan works with our Red Flag program to assure that, not only will we stop identity theft when it is being perpetrated on our customers, we will do whatever we can to avoid data breaches in the first place.

The mortgage industry has always had extensive checks and balances in place to assure the identities of our customers and their records are accurate. To facilitate that the following quality control modules are incorporated by reference. Throughout this document we will reference policies and procedures that are part of our normal business operations, but rightfully belong in other areas of our organizational documentation. These areas are:

- Origination
- Processing
- Underwriting
- Closing
- Quality Control and Compliance
- Physical Operations and Human Resources
- Wholesale Operations

Information Security

We are expected to have an identity theft program in place. This is to assure that in addition to helping consumers identify risks we do not contribute to the problem. There are many areas in which Company Name collects and exchanges private financial information in the course of our daily business. The information security portion of our plan is designed to assure that we have safeguards in place to prevent loss of information and to define how we respond in the even of a data breach.

Federal Laws

The increase of identity theft as a crime in the United States has been accompanied by an increase in the number of laws designed to protect consumers. All of the credit related laws are organized under Regulation B the Equal Credit Opportunity Act. More specifically The Gramm-Leach-Bliley Financial Privacy Act, the Fair Credit Reporting Act, and the Fair and Accurate Credit Transactions Act, all guide us in our policy development. In addition, the Sarbanes-Oxley Act is applicable as it applies to document retention and destruction.

Beyond Compliance

We believe that protecting consumer's information is not only a responsibility, but can help us increase our business. By proactively reaching out to consumers and educating those consumers about information security and identity theft, we can increase the level of trust the public places in us. This will result in an increased level of business.

Section 1 - Understanding Information Security and Identity Theft

Identity theft in the United States

The Federal Trade Commission (FTC) commissions regular studies on identity theft, most recently in 2005. In 2006 they released the results which estimated that there were approximately 8.3 million victims of identity theft and the United States in 2005. Compared to the 2002 study this might indicate that identity theft was on the decline. An estimated 10 million victims were reported in 2002. In addition, the survey estimated that $15.6 billion were lost and 2006. This compares to $7.6 billion in the 2003 survey. While, according to The Javelin Group a research firm, identity theft has decreased somewhat since that time because of the increased awareness of the problem, the numbers are still staggering.

When examining identity theft the Federal Trade Commission surveys break the incidents into three categories: 1.) existing credit card users, 2.) existing non credit card accounts, and 3.) new accounts and other frauds. This is important to Company Name because we are not credit card issuers – we only see fraud in the mortgage lending environment.

Identity Theft vs. Identity Fraud

There is a difference between identity theft and identity fraud. Identity theft is when personal information is accessed without your permission. Identity fraud is when that information is used to commit a crime for financial gain.

Common Identity Theft Scenarios

Shoulder surfing is when a criminal witnesses a transaction being conducted and gathers the personal information necessary to repeat that transaction later.

Often identity theft occurs by members of family and friends, or company employees.

Many consumers often volunteer their personal financial information over the Internet and online identity theft is one of the areas that is of the greatest concern.

"Vishing" is a telephone based version of the online "phishing." Persons contact consumers by telephone and attempt to trick the consumer into providing personal financial information.

Table 1: Prevalence of ID Theft in 2005, by Category of Misuse

	Percent of Adult Population[1]	Number of Persons (millions)[2]
New Accounts & Other Fraud	0.8 % (0.5 % - 1.2%)	1.8 (1.2 – 2.8)
Misuse of Existing Non-Credit Card Account or Account Number	1.5 % (1.1% - 2.1%)	3.3 (2.4 – 4.6)
Misuse of Existing Credit Card or Credit Card Number	1.4 % (1.0 % - 2.1%)	3.2 (2.1 – 4.6)
Total Victims in 2005	3.7 % (3.0% - 4.6%)	8.3 (6.6 – 10.3)

For the mortgage industry, and the financial services industry in general, data breaches are the area of biggest concern. Data breaches occur when large amounts of personal information are accessed from outside of the firm. Although surveys report that data breaches generally result in the smallest percentage of identity fraud situations, the potential for massive losses cause this to be the largest focus of the company's information security plan.

2006 Identity Theft Survey Report Page -17-

Figure 4 – Q1 / Q29 - Existing Accounts Misused[4]

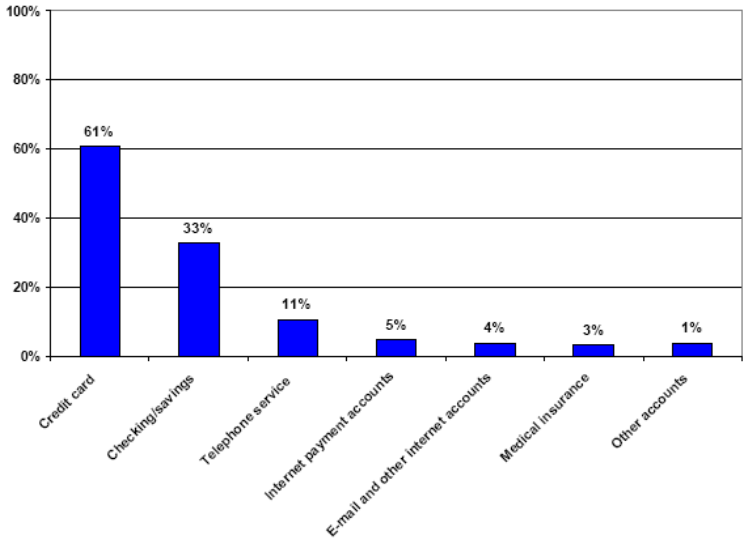
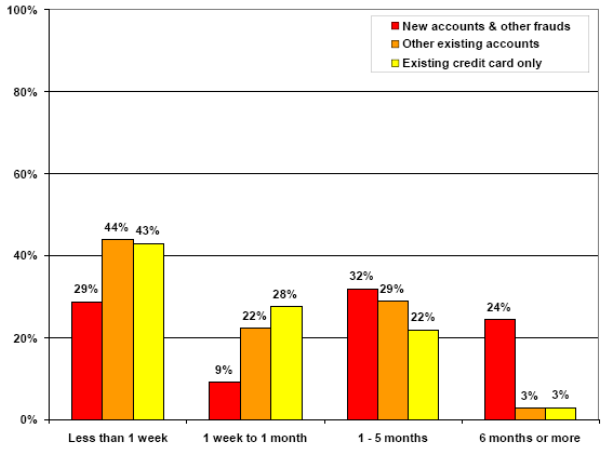


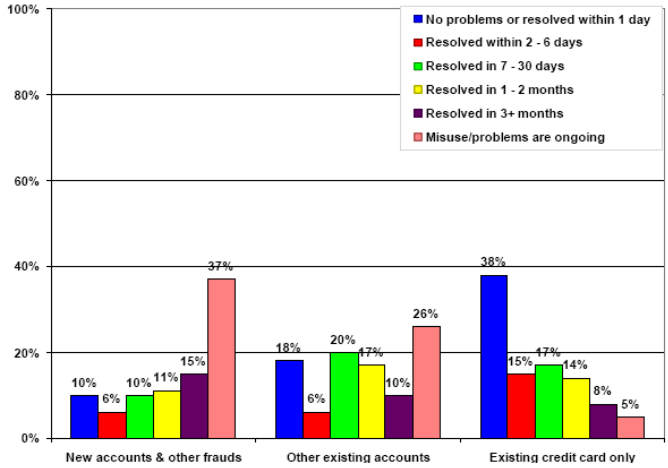
Figure 7 - Q16 – Length of Time to Discover Misuse[11]



Identifying Potential Fraud Quickly

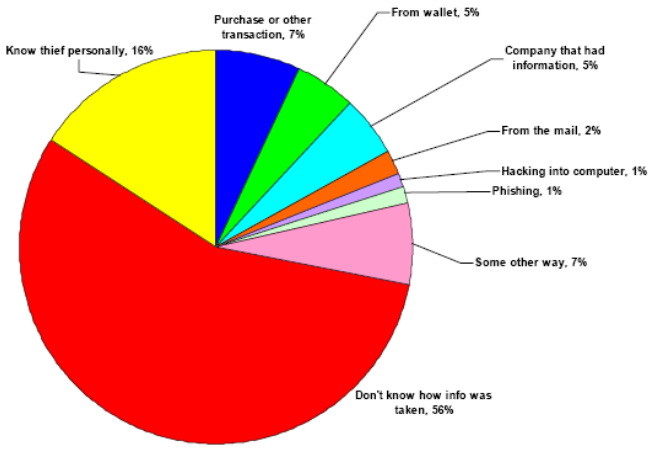
Nearly a quarter (25%) of all new account another fraud victims did not find out about the misuse of their information and time the six months after it started compared to just 3% of existing credit card users. This is the rationale for having a "red flag" system of identity theft detection. The sooner the crime is discovered the more quickly and losses can be prevented.

Figure 8 - Q17 / Q19 / Q20 – Problem Resolution[13]



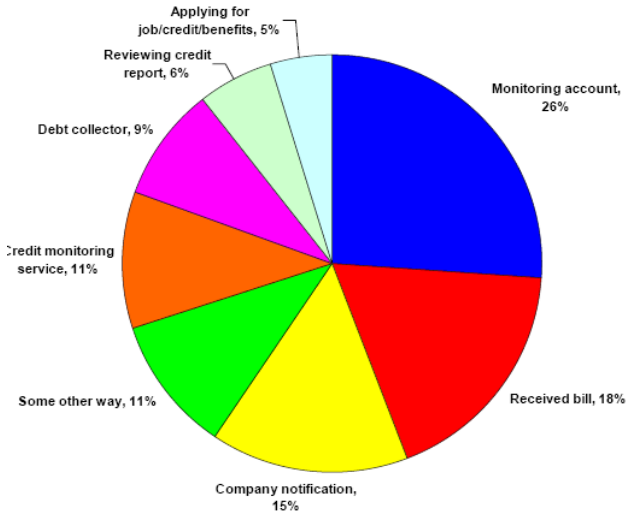
Identity fraud is a pernicious crime. Once discovered, particularly when perpetrated on new accounts, the problems tend to be ongoing. This is because they continue to affect other areas of credit, including the mortgage application process.

Figure 10 - Q23 / Q25 / Q26 / Q27 – How Information Was Obtained[16]



Most consumers don't know how their personal information was accessed. This lends credence to the idea that we have a proactive information security, and red flag, land in place to alert consumers if there is a breach of data, or somebody opens up an account without their knowledge.

Figure 11 - Q21 / Q21a – How Victims Discovered ID Theft[18]



Since only a small percentage of all consumers have credit monitoring services, discovery of the theft is more likely to occur on an existing account. The customer receives a bill sees unauthorized transactions, and makes a report. However if the account of our identity theft results in a new account, without outside information the consumer has little or no way of discovering identity theft and identity fraud.

Section 2 - Information Security Plan

Introduction

Information security is the protection of the data that we keep on our premises and systems in the normal course of our business. In addition to Company Name's private company information, there is the valuable personal information of our customers, borrowers and applicants. We have an obligation under federal law to keep that information safe.

Our Information Security Plan has the following components

- Securing Personal Information
- Destruction of Secure Information and Records
- Remediation in the Event of a Breach

Areas of Risk

The risk of large scale data theft is normally targeted towards larger institutions that may have a larger customer base and consequently have a greater opportunity for reward. Again, the average credit card identity fraud theft results in losses of less than $1,000. Unfortunately, mortgage offices, while they offer smaller scale opportunities for theft, also represent financial assets of far greater value. One theft can result in hundreds of thousands of dollars of losses. We require safeguards at all levels.

Authorized Personnel

All staff members are required to complete an employment initiation process which includes background check and education in the areas of general company policy, regulations and information security. Temporary staff, contractors and non-employee staff may not access customer information without clearance.

Office Security

During hours of operation, attended doors may be left open. However, should the door be unattended, replacement reception personnel must be arranged, or the door must be locked and signage placed reading "Reception Area Unattended, please ring for entry." Bonded cleaning crews may be allowed to clean the office space after hours.

Guests must be escorted by an employee at all times. Guests must sign in at the reception area.

Side doors and fire doors may not be propped open. Signage must be in place that reads "KEEP DOOR LOCKED AT ALL TIMES."

A person leaving his or her desk must replace all files and lock them in secure desk or filing cabinet drawers.

Clean Desk Policy

An effective clean desk effort involving the participation and support of all Company Name employees can greatly protect paper documents that contain sensitive information about our clients, customers and vendors. All employees should familiarize themselves with the guidelines of this policy.

The main reasons for a clean desk policy are:

A clean desk can produce a positive image when our customers visit the company.
It reduces the threat of a security incident as confidential information will be locked away when unattended.
Sensitive documents left in the open can be stolen by a malicious entity.

Responsibility

All staff, employees and entities working on behalf of company are subject to this policy

Scope

At known extended periods away from your desk, such as a lunch break, sensitive working papers are expected to be placed in locked drawers.At the end of the working day the employee is expected to tidy their desk and to put away all office papers. Company Name provides locking desks and filing cabinets for this purpose.

Action

- Allocate time in your calendar to clear away your paperwork.
- Always clear your workspace before leaving for longer periods of time.
- If in doubt - throw it out. If you are unsure of whether a duplicate piece of sensitive documentation should be kept - it will probably be better to place it in the shred bin.
- Consider scanning paper items and filing them electronically in your workstation.
- Use the recycling bins for sensitive documents when they are no longer needed.
- Lock your desk and filing cabinets at the end of the day
- Lock away portable computing devices such as laptops or PDA devices
- Treat mass storage devices such as CDROM, DVD or USB drives as sensitive and secure them in a locked drawer

Enforcement

Any employee found to have violated this policy may be subject to disciplinary action, up to and including termination of employment.

Laptop Computers and Mobile Devices

This describes Information Security requirements for encrypting data at rest on Company Name mobile devices.

This policy applies to any mobile device issued by Company Name or used for Company Name business which contains stored data owned by Company Name.

All mobile devices containing stored data owned by Company Name must use an approved method of encryption to protect data at rest. Mobile devices are defined to include laptops, PDAs, and cell phones.

Users are expressly forbidden from storing Company Name data on devices that are not issued by Company Name, such as storing Company Name email on a personal cell phone or PDA.

Laptops must employ full disk encryption with an approved software encryption package. No Company Name data may exist on a laptop in cleartext.

PDAs and Cell phones

Any Company Name data stored on a cell phone or PDA must be saved to an encrypted file system using Company Name-approved software. Company Name shall also employ remote wipe technology to remotely disable and delete any data stored on a Company Name PDA or cell phone which is reported lost or stolen.

Keys

All keys used for encryption and decryption must meet 128 bit complexity requirements.

Loss and Theft

The loss or theft of any mobile device containing Company Name data must be reported immediately.

Enforcement

Any employee found to have violated this policy may be subject to disciplinary action, up to and including termination of employment.

Definitions

Term	Definition
Cleartext	Unencrypted data
Full disk encryption	Technique that encrypts an entire hard drive, including operating system and data
Key	Phrase used to encrypt or decrypt data

PDA	Personal Data Assistant.
Remote wipe	Software that remotely deletes data stored on a mobile device.

Desktop Security Policy

The purpose of this policy is to provide guidance for workstation security for Company Name workstations in order to ensure the security of information on the workstation and information the workstation may have access to.
Scope

This policy applies to all Company Name employees, contractors, workforce members, vendors and agents with a Company Name-owned or personal-workstation connected to the Company Name network.

Policy

Appropriate measures must be taken when using workstations to ensure the confidentiality, integrity and availability of sensitivity information, and that access to sensitivity information is restricted to authorized users.

Workforce members using workstations shall consider the sensitivity of the information, that may be accessed and minimize the possibility of unauthorized access. Company Name will implement physical and technical safeguards for all workstations that access electronic protected health information to restrict access to authorized users.

Appropriate measures include:

- Restricting physical access to workstations to only authorized personnel.
- Securing workstations (screen lock or logout) prior to leaving area to prevent unauthorized access.
- Enabling a password-protected screen saver with a short timeout period to ensure that workstations that were left unsecured will be protected
- Complying with all applicable password policies and procedures.
- Ensuring workstations are used for authorized business purposes only.
- Never installing unauthorized software on workstations.
- Storing all sensitivity information on network servers
- Keeping food and drink away from workstations in order to avoid accidental spills.
- Securing laptops that contain sensitivity information by using cable locks or locking laptops up in drawers or cabinets.
- Complying with the Portable Workstation Encryption policy
- Complying with the Anti-Virus policy
- Ensuring that monitors are positioned away from public view. If necessary, install privacy screen filters or other physical barriers to public viewing.

- Ensuring workstations are left on but logged off in order to facilitate after-hours updates. Exit running applications and close open documents
- Ensuring that all workstations use a surge protector (not just a power strip) or a UPS (battery backup).
- If wireless network access is used, ensure access is secure by following the Wireless Access policy

Enforcement

Any employee found to have violated this policy may be subject to disciplinary action, up to and including termination of employment.

Definitions

Workstations include: laptops, desktops, PDAs, computer based medical equipment containing or accessing patient information and authorized home workstations accessing the Company Name network.

Workforce members include: employees, volunteers, trainees, and other persons under the direct control of Company Name

Document Retention and Destruction

In accordance with the Sarbanes-Oxley Act, which makes it a crime to alter, cover up, falsify, or destroy any document with the intent of impeding or obstructing any official proceeding, this policy provides for the systematic review, retention and destruction of documents received or created by Company Name in connection with the transaction of organization business. This policy covers all records and documents, regardless of physical form, contains guidelines for how long certain documents should be kept and how records should be destroyed. The policy is designed to ensure compliance with federal and state laws and regulations, to eliminate accidental or innocent destruction of records and to facilitate Company Name's operations by promoting efficiency and freeing up valuable storage space.

Document Retention

Company Name follows the document retention procedures outlined below. Documents that are not listed, but are substantially similar to those listed in the schedule will be retained for the appropriate length of time.

Corporate Records	
Annual Reports to Secretary of State/Attorney General	Permanent
Articles of Incorporation	Permanent
Board Meeting and Board Committee Minutes	Permanent
Board Policies/Resolutions	Permanent
By-laws	Permanent
Construction Documents	Permanent
Fixed Asset Records	Permanent
IRS Application for Tax-Exempt Status (Form 1023)	Permanent
IRS Determination Letter	Permanent
State Sales Tax Exemption Letter	Permanent
Contracts (after expiration)	7 years
Correspondence (general)	3 years
Accounting and Corporate Tax Records	
Annual Audits and Financial Statements	Permanent
Depreciation Schedules	Permanent
General Ledgers	Permanent
IRS 990 Tax Returns	Permanent
Business Expense Records	7 years
IRS 1099s	7 years
Journal Entries	7 years
Invoices	7 years
Sales Records (box office, concessions, gift shop)	5 years
Petty Cash Vouchers	3 years
Cash Receipts	3 years
Credit Card Receipts	3 years

Bank Records	
Check Registers	Permanent
Bank Deposit Slips	7 years
Bank Statements and Reconciliation	7 years
Electronic Fund Transfer Documents	7 years
Payroll and Employment Tax Records	
Payroll Registers	Permanent
State Unemployment Tax Records	Permanent
Earnings Records	7 years
Garnishment Records	7 years
Payroll Tax returns	7 years
W-2 Statements	7 years
Employee Records	
Employment and Termination Agreements	Permanent
Retirement and Pension Plan Documents	Permanent
Records Relating to Promotion, Demotion or Discharge	7 years after termination
Accident Reports and Worker's Compensation Records	5 years
Salary Schedules	5 years
Employment Applications	3 years
I-9 Forms	3 years after termination
Time Cards	2 years
Loan Application Copy File	3 years after completion
Loan Servicing File	3 years after loan payoff

Electronic Documents and Records

Electronic documents will be retained as if they were paper documents. Therefore, any electronic files, including records of donations made online, that fall into one of the document types on the above schedule will be maintained for the appropriate amount of time. If a user has sufficient reason to keep an email message, the message should be printed in hard copy and kept in the appropriate file or moved to an "archive" computer file folder. Backup and recovery methods will be tested on a regular basis.

Emergency Planning

Company Name's records will be stored in a safe, secure and accessible manner. Documents and financial files that are essential to keeping Arts Organization operating in an emergency will be duplicated or backed up at least every week and maintained off site.

Document Destruction

Company Name's chief financial officer, compliance officer or general manager is responsible for the ongoing process of identifying its records, which have met the required retention period and overseeing their destruction. Destruction of financial and personnel-related documents will be accomplished by shredding.

Document destruction will be suspended immediately, upon any indication of an official investigation or when a lawsuit is filed or appears imminent. Destruction will be reinstated upon conclusion of the investigation.

Compliance

Failure on the part of employees to follow this policy can result in possible civil and criminal sanctions against Company Name and its employees and possible disciplinary action against responsible individuals. The chief financial officer and finance committee chair will periodically review these procedures with legal counsel or the organization's certified public accountant to ensure that they are in compliance with new or revised regulations.

Onsite Records Storage Policy

Active, closed or denied loan application copies, exclusive of delivery file documentation subject to the Funding, Warehousing, Delivery and Servicing Setup process, will be stored in the branch. These files will be indexed by month, and alphabetically by borrower last name. File cabinets must be locked, and keys are maintained by the operations manager and may be accessed under supervision during business hours.

Offsite Records Storage

If, due to space concerns, there is insufficient room in the branch location to provide file storage, off-site records storage may be utilized through a secure, bonded, professional records Management Company that is a member of the American Business Records Management Association. Records of each file box sent to Archive must be maintained current by the operations manager and must be available for immediate inspection within 2 hours notice.

The purpose of this policy is to ensure the proper use of Company Name's email system and make users aware of what Company Name deems as acceptable and unacceptable use of its email system. The Company Name reserves the right to amend this policy at its discretion. In case of amendments, users will be informed appropriately.

Electronic Communication

Email is a business communication tool and users are obliged to use this tool in a responsible, effective and lawful manner. Although by its nature email seems to be less formal than other written communication, the same laws apply. Therefore, it is important that users are aware of the legal risks of e-mail:

By following the guidelines in this policy, the email user can minimize the legal risks involved in the use of e-mail. If any user disregards the rules set out in this Email Policy, the user will be fully liable and Company Name will disassociate itself from the user as far as legally possible.

The following rules are required by law and are to be strictly adhered to:

- It is strictly prohibited to send or forward emails containing libelous, defamatory, offensive, racist or obscene remarks. If you receive an e-mail of this nature, you must promptly notify your supervisor.
- Do not forward a message without acquiring permission from the sender first.
- Do not send unsolicited email messages.
- Do not forge or attempt to forge email messages.
- Do not send email messages using another person's email account.
- Do not copy a message or attachment belonging to another user without permission of the originator.
- Do not disguise or attempt to disguise your identity when sending mail.

Best Practices

Company Name considers email as an important means of communication and recognizes the importance of proper email content and speedy replies in conveying a professional image and delivering good customer service. Therefore Company Name wishes users to adhere to the following guidelines:

Writing emails:

- Signatures must include your name, job title and Company Name. A disclaimer will be added underneath your signature (see Disclaimer)
- Use the spell checker before you send out an email.
- Do not send unnecessary attachments. Compress attachments larger than 200K before sending them.
- Do not write emails in capitals.
- Do not use cc: or bcc: fields unless the cc: or bcc: recipient is aware that you will be copying a mail to him/her and knows what action, if any, to take.
- If you forward mails, state clearly what action you expect the recipient to take.
- Only send emails of which the content could be displayed on a public notice board. If they cannot be displayed publicly in their current state, consider

rephrasing the email, using other means of communication, or protecting information by using a password (see confidential).
- Only mark emails as important if they really are important.

Replying to emails:

Emails should be answered within at least 8 working hours, but users must endeavor to answer priority emails within 4 hours.
Priority emails are emails from existing customers and business partners.

Newsgroups:

Users need to request permission from their supervisor before subscribing to a newsletter or news group.

Maintenance:

Delete any email messages that you do not need to have a copy of, and set your email client to automatically empty your 'deleted items' on closing.

Personal Use

Although Company Name's email system is meant for business use, Company Name allows the reasonable use of email for personal use if certain guidelines are adhered to:

- Personal use of email should not interfere with work.
- Personal emails must also adhere to the guidelines in this policy.
- Personal emails are kept in a separate folder, named 'Private'. The emails in this folder must be deleted weekly so as not to clog up the system.
- The forwarding of chain letters, junk mail, jokes and executables is strictly forbidden.
- On average, users are not allowed to send more than 2 personal emails a day.
- Do not send mass mailings.
- All messages distributed via the company's email system, even personal emails, are Company Name's property.

Confidential Information

Avoid sending confidential information by e-mail. If you do, you must secure the information by including it in a Microsoft Word, Excel or .PDF file and protect it with a password. Then provide the recipient with the password by means of other communication, for instance by telephone.

Disclaimer

The following disclaimer will be added to each outgoing email:

'This email and any files transmitted with it are confidential and intended solely for the use of the individual or entity to which they are addressed. If you have received this email in error please notify the system manager. Please note that any views or opinions presented in this email are solely those of the author and do not necessarily represent those of the company. Finally, the recipient should check this email and any attachments for the presence of viruses. The company accepts no liability for any damage caused by any virus transmitted by this email.'

System Monitoring

You must have no expectation of privacy in anything you create, store, send or receive on the company's computer system. Your emails can be monitored without prior notification if Company Name deems this necessary. If there is evidence that you are not adhering to the guidelines set out in this policy, the Company Name reserves the right to take disciplinary action, including termination and/or legal action.

Secure Fax Transmission

The legacy of fax transmission in the mortgage industry is long. The risk of using fax transmissions is that the sender has no idea whether the recipient is attending to the machine while the document is being received, printed, and then available for viewing. In order to prevent the compromise of secure information never send information to an unattended facsimile machine. If you can confirm that the recipient is standing at the machine, it is acceptable to proceed with communications in this manner.

Alternatively, we can provide an “E-fax” account for individual users. This allows the transmission of facsimiles via e-mail to a secure login account.

For transmitting paper documents, always create a password protected document and deliver the password to the recipient using a different method of communication, such as the telephone.

Secure Telephone Communications

Vishing is the criminal practice of using social engineering and Voice over IP (VoIP) to gain access to private personal and financial information from the public for the purpose of financial reward. The term is a combination of "voice" and phishing. Vishing exploits the public's trust in landline telephone services, which have traditionally terminated in physical locations which are known to the telephone company, and associated with a bill-payer. The victim is often unaware that VoIP allows for caller ID spoofing, inexpensive, complex automated systems and anonymity for the bill-payer. Vishing is typically used to steal credit card numbers or other information used in identity theft schemes from individuals.

According to the FBI's Internet Crime Complaint Center (IC3), the number of "vishing" complaints received by the center is increasing at what it calls "an alarming rate." Vishing and phishing are related, and both rely on e-mail as a means of delivering bait, but the two use different hooks in order to snag user data.

Vishing starts with an e-mail, like phishing, but requests that end-users contact a particular institution by phone in order to resolve an issue or re-secure personal data. People who call the provided number will be asked to provide the same types of data phishers attempt to procure. Ironically, vishing e-mails may even attempt to reassure recipients of their legitimacy by stating that the institution in question would never request customer financial data via e-mail or IM.

As always, the best defense against phishing or vishing is a little common sense. If your bank or other financial institution with which you are affiliated contacts you requesting personal data, hang up (or call them) using only the number provided on the back of your

card or official statement. If you can't get confirmation that the request is actually legitimate, don't follow up on it.

Social Engineering Scams – Internal and External Prevention

One of the most prevalent forms of online scams is referred to as a seemingly benign term: "social engineering." This practice, which is sometimes referred to as "phishing," refers to using trickery to get people to voluntarily hand over critical information, such as usernames or passwords.

In many cases, spam filters can easily detect the clumsier social engineering efforts and, thus, spare computer users from grief. However, there are a growing number of sophisticated efforts that are crafted to circumvent the spam filters - and unsuspecting customers that click into these cleverly disguised emails run the risk of facing serious repercussions.

Social engineering attacks mimic an email notification from a well-known and trusted source: financial institutions, LinkedIn, PayPal, the Better Business Bureau, Facebook and so forth. The attackers create an email that looks exactly like the normal system notices that are sent out by those entities, but they change the links to hit their own servers.

The most classic example is an email that sends a dire notice with a link to login and check on a potential problem. When a person clicks on the link, it takes him or her to a page on the cyberattacker's servers that looks just like the well-known entity's login page.

When a person enters his or her username and password, this information is stored in a database on the phony server while an error box appears that says, "Invalid username or password, please try again." This error box message comes with an OK button that, when clicked, redirects the person to the real login page.

People may not realize there is a problem because passwords are obscured with asterisks, so it is natural to assume there was a typo during the initial password entry. However, the miscreants now have the person's username and password.

So what does this mean to mortgage bankers if someone gets tricked into thinking a social engineering scam message really came from Facebook or LinkedIn? Quite simply, many people have the same usernames and passwords for multiple websites. Thus, a person who has unwittingly surrendered his or her personal information for a Facebook page might not realize that the social engineering scam artists could later use that information to gain access to online mortgage banking accounts.

Company Name needs to take a proactive approach in educating customers on how to identify potential scams that pop up in their email in-boxes. Here are some safety tips we send out to all customers:

1. Don't click links from emails. Instead, open a Web browser and specifically go to the site in question and login directly. It is not common for financial institutions to have a "click here to login" link within their email communications.

2. Be suspicious of serious "warnings" and dollar amounts posted directly in emails. Financial services companies are not in the habit of sending customers panic-inducing messages of "low account balances" or other account discrepancies with details plainly shown in the email. Warnings are more discreet and merely direct the customer to go log in for details.
3. Use mouse-overs to view a link before clicking. Although not all email software and hardware devices support them, a mouse-over can quickly and easily identify the links within an email message.
4. Try not to use the same password at multiple sites. Use a password program to store and remember online access data.
5. Routinely update passwords. Updating passwords, even once a year, is an easy way to stay one step ahead of the social engineering scammers.

Invite customers who are in doubt about the veracity of emails to forward them to Company Name for verification. Several sites that have been the subject of social engineering scams, including eBay and PayPal, have special email accounts that receive, review and keep track of these online frauds. These spoof-checking efforts will help empower the customer to ensure that Company Name does not become the victim of the next big Internet fraud.

Data Breach Policy Implementation Guide

The response to any breach of personally identifiable information (PII) can have a critical impact on the Company Name's reputation and how trustworthy the public perceives the company. Thus, exceptional care must be taken when responding to data breach incidents. Not all incidents result in data breaches, and not all data breaches require notification. This guide is to assist the Data Breach Team in developing an appropriate response to a data breach based on the specific characteristics of the incident.

Background

This Data Breach Policy Implementation Guide is based on the President's Identity Theft Task Force recommendations that provide a menu of steps for the company to consider, so that it may pursue a risk-based, tailored response to data breach incidents.

Definition of Breach

A breach is a loss of control, compromise, unauthorized disclosure, unauthorized acquisition, unauthorized access, or any similar term referring to situations where persons other than authorized users and for an authorized purpose have access or potential access to PII in usable form, whether physical or electronic.

Reporting Breaches and Breach Response Team

Breach is immediately reported to

- Chief Privacy Officer (CPO)
- Chief Information Officer (CIO)
- Chief, IT Security Office (ITSO)
- Associate Director for Communications
- Chief, Office of Analysis and Executive Support (OAES)
- As warranted:
- Chief, Office of Security
- General Counsel
- Law Enforcement

Risk Assessment Process

Risk is a function of the probability or likelihood of a privacy violation, and the resulting impact of that violation. To assign a risk score, assess the probability of the event (data breach) occurring and then assess the impact or harm caused to an individual and our organization in its ability to achieve its mission.

Likelihood	Likelihood Definition
High (H)	The nature of the attack and the data indicate that the motivation is criminal intent; the security of the data and controls to minimize the likelihood of a privacy violation are ineffective.
Medium (M)	The nature of the attack and data indicate that the motivation could be criminal intent; but controls are in place that may impede success.
Low (L)	The nature of the attack and data do not indicate criminal intent, and security and controls are in place to prevent, or at least significantly impede, the likelihood of a privacy violation.

To assess likelihood of a breach occurring, consider five factors:
1. How the loss occurred
2. Data elements breached
3. Ability to access the data - the likelihood the personal information will be or has been compromised – made accessible to and usable by unauthorized persons
4. Ability to mitigate the risk of harm
5. Evidence of data being used for identity theft or other harm

1. How Loss Occurred
H - Online system hacked
H - Data was targeted
M - Device was targeted
M - Device stolen
L - Device lost

2. Data Elements Breached*
H - Social Security Number
H - Biometric record
H - Financial account number
H - PIN or security code for financial account
H - Health data
M - Birthdate
M - Government Issued Identification Number (drivers license, etc.)
L - Name
L - Address
L - Telephone Number
*A combination of identifying information and financial or security information should always be considered a high risk with high likelihood of harm occurring.

3. Ability to access data
H – paper records or electronic records in a spreadsheet that is not password protected
M – electronic records that are password protected only
L – electronic records that are password protected and encrypted

4. Ability to mitigate the risk of harm
H – no recovery of data
M – partial recovery of data

L – recovery of data prior to use

5. Evidence of data being used for identity theft or other harm
H – Data published on the web
M – Data accessed but no direct evidence of use
L – No tangible evidence of data use

After evaluating each factor and assigning an overall probability or likelihood of a breach occurring, review and assess the impact or harm to an individual or our organization.

Impact Rating	**Impact Definition**
High	Event (1) may result in human death or serious injury or harm to individual; (2) may result in high costs to organization; or (3) may significantly violate, harm, or impede an organization's mission, reputation, or interest.
Medium	Event (1) may result in injury or harm to the individual; (2) may result in costs to the organization; or (3) may violate, harm, or impede an organization's mission, reputation, or interest.
Low	Event (1) may result in the loss of some tangible organizational assets or resources; or (2) may noticeably affect an organization's mission, reputation, or interest.

The impact depends on the extent to which the breach poses a risk of identity theft or other substantial harm to an individual such as: embarrassment, inconvenience, unfairness, harm to reputation or the potential for harassment or prejudice, particularly when health or financial benefits information is involved.

Financial considerations can be factored in when determining the impact on our organization. For instance, credit monitoring is generally estimated at $20 per year per case (individual). The costs associated with implementing a call center including staff salaries may also be a factor. Alternatively, the cost of contracting for this service could be a factor.

Assigning Risk Score

The risk score is determined by cross-referencing the likelihood score with the impact score.

Likelihood	Impact		
	Low	Medium	High
High	Medium	High	High
Medium	Low	Medium	High
Low	Low	Low	Medium

Notification of Individuals

The risk score assigned will help determine if and when we should provide notification. If the likelihood of risk is low, there could be more harm or impact on the individual if notification is provided due to the actions the notified individual may take. Thus, notification must be weighed with the likelihood of risk. No notification may be required when the risk levels of each of the five factors is low. If the likelihood of risk is high and the level of impact or harm to the individual is medium, notification and remedy may be required. Alternatively, if the likelihood of risk is low and the level of impact or harm to the individual is high, notification only may be required. If the five factors are considered appropriately, it is more likely that notification will only be given in those instances where there is a reasonable risk of harm and will not lead to the overuse of notification and thus the associated further complications to the individual.

Thus, consideration should be given to all factors when determining final actions to take when addressing each incident. The table below should only be used as guide and conditions may warrant actions above or below those associated with the final risk score.

Risk Score	Necessary Action
High	Notify and provide remedy
Medium	Notify only
Low	Monitor only

Timing of Notification

Notice will be provided within a reasonable time following the discovery of a breach consistent with the legitimate needs of law enforcement and any measures necessary for the Census Bureau to determine the scope of the breach and, if applicable, to restore the reasonable integrity of the system/process that was compromised.

In some circumstances, law enforcement considerations may require a delay in notification if the investigation of the breach or of an individual affected by the breach requires it and notification would seriously impede the investigation. The delay should not exacerbate risk or harm to any affected individual(s) or be tied to the completion of

the investigation, but rather be based on whether it would seriously impede the investigation to provide the notice promptly.

Responsibility for Notification

The notice should come from a senior Company Name representative.

Content of Notification

The notice must be clear, concise, conspicuous, easy-to-understand, in plain language and should include the following elements:

- A brief description of what happened, including the date(s) of the breach and its discovery.
- A description of the types of personal information that were involved in the breach (e.g., full name, Social Security number, date of birth, home address, account number, disability code, etc.) to the extent possible.
- What steps, if any, an individual should take to protect himself from potential harm.
- What Company Name is doing, if anything, to investigate the breach, to mitigate losses, and to protect against any further breaches.
- Who and how affected individuals should contact Company Name for more information, including a toll-free telephone number, e-mail address, and postal address.
- Direction to additional guidance available from the Federal Trade Commission at: http://www.consumer.gov/idtheft/.

Minimizing your risk at: http://www.consumer.gov/idtheft/con_minimize.htm.
Publications at: http://www.consumer.gov/idtheft/con_pubs.htm.

Method of Communication

Notice of the breach will be provided commensurate to the number of individuals affected by the breach and the availability of contact information Company Name has for the affected individuals. Correspondence must be prominently marked on the exterior reflecting the importance of the communication to help ensure the recipient does not discard or otherwise ignore the notification.

In general, the primary means of notification will be by first-class mail to the last known mailing address of the individual based on Company Name records.

Where we have reason to believe that the address is no longer current, reasonable efforts will be made to update the address using the U.S. Postal Service National Change of Address (NCOA) database.

Substitute notice **may** be made in instances where Company Name does not have sufficient contact information for those who need to be notified. In such instances, notice **may** consist of a conspicuous posting of the notice on the company's home page of its web site and include additional information in a Frequently Asked Questions (FAQ).

Process for Remediation of a Breach

Remedy is provided when the risk score is High.

Credit Monitoring Data Breach Risk Packages (i.e. Lifelock)

Low Risk Package	Low Risk Package Includes: Social Security, Credit Card and 1 Bureau Credit Report Monitoring 3 Bureau Initial Fraud Alert Credit Card Registry Online Identity Theft Assistance 24 x 7 Customer Support
Medium Risk Package	Medium Risk includes Low Risk benefits plus: Instant 1 Bureau Credit Report Instant 1 Bureau Credit Score Personal Information Directory Monitoring and Deletion Identity Theft Consumer Guide $25,000 ($0 deductible) Identity Theft Insurance
High Risk Package	High Risk includes Medium Risk benefits plus: 3 Bureau Credit Report Monitoring Instant 3 in 1 Credit Report Instant 3 Bureau Credit Scores Fraud Resolution & Identity Restoration Specialist

Reporting a Data Breach

Security Breach Notification Laws have been enacted in most U.S. states since 2002. These laws were enacted in response to an escalating number of breaches of consumer databases containing personally identifiable information. The first such law, the California data security breach notification law was enacted in 2002 and became effective on July 1, 2003. As related in the bill statement, law requires "a state agency, or a person or business that conducts business in California, that owns or licenses computerized data that includes personal information, as defined, to disclose in specified ways, any breach of the security of the data, as defined, to any resident of California whose unencrypted personal information was, or is reasonably believed to have been, acquired by an unauthorized person." In addition the law permits delayed notification "if a law enforcement agency determines that it would impede a criminal investigation." The law also requires any entity that licenses such information to notify the owner or licensee of the information of any breach in the security of the data.

The California law has been the model for the enactment of similar laws in other states. The National Conference of State Legislatures maintains a list of enacted and proposed security breach notification laws

State	Time To Notify Consumers of a Breach of Personal Information	Civil or Criminal Penalties for Failure to Promptly Notify Customers of Breach	Private Right of Action	Exemption for Encrypted Personal Info	Exemption for Criminal Investigations or Information Publicly Available from Government Entities	Exemption for Immaterial Breaches
Arizona	Most expedient time possible, without unreasonable delay	●		●	●	
Arkansas	Most expedient time possible, without unreasonable delay	●		●	●	●
California	Most expedient time possible, without unreasonable delay		●	●	●	
Colorado	Most expedient time possible, without unreasonable delay	●		●	●	●
Connecticut	Immediately			●	●	●
Delaware	Immediately, in the most expedient time possible, without unreasonable delay	●	●	●	●	
District of Columbia	Most expedient time possible, without unreasonable delay	●	●		●	
Florida	Without unreasonable delay	●		●	●	
Georgia	Most expedient time possible, without unreasonable delay			●	●	
Hawaii	Without unreasonable delay	●	●	●	●	
Idaho	Most expedient time possible, without unreasonable delay	●		●	●	●
Illinois	Most expedient time possible, without unreasonable delay		●	●	●	
Indiana	Without unreasonable delay			●	●	
Kansas	Most expedient time possible, without unreasonable delay	●		●	●	●
Louisiana	Most expedient time possible, without unreasonable delay		●		●	●
Maine	As expediently as possible, without unreasonable delay	●		●	●	
Maryland	As soon as reasonably practicable	●	●	●	●	●
Massachusetts	As soon as practicable and without unreasonable delay.	●		●	●	●
Michigan	Without unreasonable delay	●		●	●	●
Minnesota	Most expedient time possible, without unreasonable delay	●		●	●	
Montana	Without unreasonable delay	●		●	●	
Nebraska	Without unreasonable delay	●		●	●	●

State	Time To Notify Consumers of a Breach of Personal Information	Civil or Criminal Penalties for Failure to Promptly Notify Customers of Breach	Private Right of Action	Exemption for Encrypted Personal Info	Exemption for Criminal Investigations or Information Publicly Available from Government Entities	Exemption for Immaterial Breaches
Nevada	As soon as possible, without unreasonable delay	●	● *	●	●	
New Hampshire	As soon as possible.					
New Jersey	Most expedient time possible, without unreasonable delay			●	●	●
New York	Most expedient time possible, without unreasonable delay	●				
North Carolina	Without unreasonable delay	●	●		●	●
North Dakota	Most expedient time possible, without unreasonable delay			●	●	
Ohio	Most expedient time possible, but not later than 45 days	●			●	●
Oklahoma	Most expedient time possible, without unreasonable delay			●	●	
Oregon	Most expedient time possible, without unreasonable delay	●		●	●	●
Pennsylvania	Without unreasonable delay	●		●	●	
Rhode Island	Most expedient time possible, without unreasonable delay	●	●	●	●	●
Tennessee	Most expedient time possible, without unreasonable delay		●	●	●	
Texas	As quickly as possible	●			●	
Utah	Most expedient time possible, without unreasonable delay	●		●	●	●
Vermont	Most expedient time possible, without unreasonable delay	●		●	●	●
Washington	Most expedient time possible, without unreasonable delay		●	●	●	●
Wisconsin	Within a reasonable time, not to exceed 45 days				●	
Wyoming	As soon as possible, in the most expedient time possible and without unreasonable delay	●			●	●

* The private cause of action is assigned to the data collector whose information was breached against the party responsible for the breach.

Section 3 - Red Flag Identity Theft Program – Covered Transactions

Covered Transactions - Defined

The Federal regulations define a covered account as:

(i) An account that a financial institution or creditor offers or maintains, primarily for personal, family, or household purposes, that involves or is designed to permit multiple payments or transactions, such as a credit card account, mortgage loan, automobile loan, margin account, cellphone account, utility account, checking account, or savings account; and
(ii) Any other account that the financial institution or creditor offers or maintains for which there is a reasonably foreseeable risk to customers or to the safety and soundness of the financial institution or creditor from identity theft, including financial, operational, compliance, reputation, or litigation risks.

As providers of mortgage loan services, Company Name is subject to the red flag rules, and our applicants meet the definition of "customers".

High Risk Entities and Practices

In general, high-risk entities may provide consumer financial services or other goods or services of value to identity thieves such as telecommunication services or goods that are easily convertible to cash, whereas low-risk entities may do business primarily with other businesses or provide non-financial services or goods that are not easily convertible to cash. By this definition, we do not provide services or goods that are easily converted to cash.

Company Name has maintained a fraud prevention program as part of our usual and customary business practices and already takes steps to minimize losses due to fraud. According to the Federal Trade Commission (FTC) ruling on the Red Flag Program Requirements, only relevant staff need be trained to implement the Program, as necessary. Staff already trained as a part of a covered entity's anti-fraud prevention efforts do not need to be re-trained except as incrementally needed.

The Education program the FTC sees as appropriate requires approximately 4 hours in the year of implementing the program, and that there should be approximately 1 hour per year of recurring education. Company Name must maintain this written program.

Mortgage Fraud and Identity Theft

The provisions of the FTC's "Red Flag Identity Theft Guidelines" state that covered entities that already perform elements of an identity theft program – such as in a complete

fraud prevention quality control plan – do not have to have separate training programs in red flag identity theft prevention.

The elements of the Company Name's Fraud Prevention Program are incorporated by reference here. Further specific elements are addressed in subsequent sections of this plan – "Red Flag Identification" at specific stages of the origination process.

Risk from Referral Sources

In a business to business sales environment it is typical to exchange some elements of a consumer's private information. All outside sales representatives should establish a list of referral sources and ascertain that the referral source's firm has an information security plan and Red Flag identity theft program in place.

Section 4 – Vendors and Vendor Approval Process

Risk from Vendors

In Company Name's interaction with vendors the greatest risk posed to the consumers' private financial information is at the time the file physically moves from our office to the office of the outside vendor. In each of these cases care needs to be taken to ensure that we are aware of which private information is being disclosed in the degree to which it could be subject to data breach.

These potential breaches occur primarily with our main vendor groups; credit bureaus, appraisers, private mortgage insurance companies, and outside investors. While we focus on these individual groups, any company that has access to our records needs to be considered as a risk factor.

We grade the risk on two factors from our own information safeguard criteria:

The risk based on the information that is shared
The risk based on the information security plan of the vendor

Level of Risk (High, Medium or Low)	**Data Elements***
H	Social Security Number
H	Biometric record
H	Financial account number
H	PIN or security code for financial account
H	Health data
M	Birth date
M	Government Issued Identification Number (driver's license, etc.)
L	Name
L	Address
L	Telephone Number
*A combination of identifying information and financial or security information should always be considered a high risk with high likelihood of harm occurring.	

Company Name
Approved Vendor Application

To be considered as an Approved Vendor for Your Company Name Here, please complete the following application and provide the requested documentation

Contact Name in Full:			Age:		Phone: ( )
Company Name:					Fax: ( )
Business Address:					
City:	County:		State:	Zip:	E-mail:
Do you carry liability insurance?	Yes	No	If yes, name of carrier:		
Amount of coverage: $					
Title Insurance Companies Only					
Are you presently under contract as an agent for a title company? Yes No			For what companies are you an agent?		
If yes, do you issue commitments?	Yes	No	Do you issue policies?	Yes	No
All Vendors					
Do you have a "Red Flag" and Private Information Security Plan? If yes, how often do you update risks and procedures?					
Name of Reference 1:			Phone:		
Name of Reference 2:			Phone:		
Name of Reference 3:			Phone:		

Please attach:

(___) Copy of Liability Policy Declarations Page
(___) Copy of Insured Closing Protection Letter from all Title Companies through which you write policies
(___) Specific Bank Wiring Instructions

Approved Vendor Application
10/5/2008

Red/Flag Information Security Program

Vendor Clearance

Name	Type	Date Requested	Confirmed	Verified by

Information Transfer to Investors and Private Mortgage Insurance Companies

Whenever possible files and should be transferred electronically via imaging software protocol. Often physical exhibits are transferred to the investor for review by underwriting. When this occurs we must be sure that the investor has information privacy and red flag detection program in place.

Responsible Party	Step	Description
Operations manager	Request confirmation investor has information security policy	No further investigation is required upon confirmation of red flag policy in place
Outside investor compliance officer	Provide verbal confirmation of red flag policy	
Processor, loan originator, underwriter	Deliver documentation via secure method	Choose secure delivery format-Federal express, UPS, or other Address specific individual Request signature confirmation

Risk Level

HIGH

Information Transfers to Credit Bureaus

Of all the vendors we would expect to have a documented plan, credit bureaus are the most sensitive information providers. The flow of sensitive information-debt payoff re-certifications, loan payment histories, and alternative payment history verifications just to name a few-is very rapid between lenders and credit bureaus. Company Name provides secure methods of communication, via e-mail, secure fax, and telephone.

Credit Bureau Risk Assessment

HIGH

Information transfers to Appraisers

Of all of our information transfers to vendors appraisers represent the lowest risk. This is because the only information that is normally transmitted is the borrower's name, address and telephone information. Care should be taken when making requests on agency loans where additional information, such as the social security number of the applicant may be revealed.

The ordinary process for requesting appraisals normally involves sending an appraisal request form via facsimile. Any secure information should be sent utilizing a secure method specifically password protected a facsimile, or a word document containing a password protection.

"House Stealing"

A recent phenomenon in some areas of the country is the fraud scheme which is known as "house stealing". This scheme involves the transfer and sale of one property without the current owner's knowledge. You may be alerted to a scheme like this through the appraiser, who indicates that the occupant or owner was unaware that the property was for sale or being refinanced.

Appraiser Risk Assessment

MEDIUM

Information Transfer to Attorneys and Title Companies

The most vulnerable time for information to be lost is right after the loan closes. Information is being transferred electronically, by fax or even hand carried by the closing agent.

Closing Agent Risk Assessment

HIGH

Section 5 - Identity Theft "Red Flags"

There are 26 red flags that the Federal trade commission has identified. They fall into five basic groups. These red flags function as guidelines. We have identified which functions these specific red flags applied to and have incorporated them into our overall fraud prevention program.

While it is clear that some of the standard red flag issues apply specifically to the credit card business, there are elements of Company Name's business that do involve revolving credit. In addition, there are red flags that applied to the loan servicing element of our business. We have assembled this matrix, from the Federal guidelines, to determine which areas we need to incorporate red flag guidance into our own procedures.

Victim or Perpetrator?

Some of these red flags made be an indication that the consumer has been a victim of identity theft. Others may be an indication that our customer may be trying to perpetrate identity theft or other fraud.

Red flag	Description - Applicability to	Applicable
A fraud alert included with a consumer report.	If the consumer credit report indicates a fraud alert, it is possible that the customer is already aware of potential identity theft issues. Conversely, the fraud alert may indicate a possible identity theft in progress.	Origination Processing
Notice of a credit freeze in response to a request for a consumer report.	A consumer's redress in the event of the notification of the disease that is to "freeze" his or her credit report. This means that the customer should be able to provide a "PIN" which would allow the "unfreezing" of the account for the mortgage lenders purposes. The customer who is unable to provide the "PIN" is probably attempting mortgage identity theft fraud	Origination
A consumer reporting agency providing a notice of address discrepancy.	The credit bureau reporting an address discrepancy may indicate that the borrower has multiple addresses, or is attempting to perpetrate occupancy fraud.	Origination Processing
Unusual credit activity, such as an increased number of accounts or inquiries.	Multiple inquiries are a warning sign normally addressed in the credit scoring process, but also by the processor in evaluating the creditworthiness of the applicants. Multiple inquiries must be addressed in writing. This process in itself is a red flag alert process on behalf of the borrower	Origination Processing Underwriting
Documents provided for identification appearing altered or forged.	Identification fraud will generally present itself at application. The applicant may provide documents in evidence of citizenship, Social Security identification, or other photo identification for the patriot act purposes.	Origination Processing Underwriting
Photograph on ID inconsistent with appearance of customer.		

Red flag	Description - Applicability to	Applicable
Information on ID inconsistent with information provided by person opening account.		
Information on ID, such as signature, inconsistent with information on file at financial institution.	With more loans requiring full documentation, we have more opportunities to verify signatures. During the direct documentation request process, a signature authorization is sent to the bank for listed on the application for verification of the information listed. The bank or other verifying entity will Compare signatures and will refuse the verification if they don't match. If full copy tax returns are found in file, it is relatively simple to compare signatures on the tax returns with the signatures on the application.	Processing Underwriting
Application appearing forged or altered or destroyed and reassembled.	Mortgage lenders generally do not accept applications which have been altered it or assembled in any way. In addition, the application process is normally supervised by a loan originator, in the literature must affix his or her signature to the application document. This process makes it impossible to intercept and manipulate application forms. This particular red flag was designed for mail out pre-approved credit card applications.	N/A Inbound call center
Information on ID not matching any address in the consumer report, Social Security number has not been issued or appears on the Social Security Administration's Death Master File, a file of information associated with Social Security numbers of those who are deceased.	In addition to our general checks of fraudulent information relative to Social Security our ability, mortgage credit report vendors who utilize Equifax, Experian and TransUnion will receive an alert, either through Safescan, FACS, or Hawk Alert that there is more than one variance for any facet of the customer's identification profile.	Origination Processing Underwriting
Lack of correlation between Social Security number range and date of birth.		
Personal identifying information associated with known fraud activity.	When any address, employment, or banking and financial information reflects an address that is a temporary mailbox, there is an obvious correlation with fraud activity being perpetrated by the applicants. The perpetrator is trying to avoid alerting the identity theft of victim by utilizing fictitious addresses.	Origination Processing Underwriting
Suspicious addresses supplied, such as a mail drop or prison, or phone numbers associated with pagers or answering service.		
Social Security number provided matching that submitted by another person opening an account or other customers.	Mortgage lenders do not normally utilize social security numbers for opening accounts. The length of the mortgage verification process normally precludes a quick over utilization of a Social Security number. In addition Safescan, FACS, or Hawk Alert will normally alert to this activity.	Servicer

Red flag	Description - Applicability to	Applicable
An address or phone number matching that supplied by a large number of applicants.	For smaller lenders, application intake would not necessarily trigger overview of identification information matching other applicants.	Servicer
The person opening the account unable to supply identifying information in response to notification that the application is incomplete.	Normal verification of the application results in a request for additional information. Often this information is quite sophisticated, and generally is requested in writing.	Processing Underwriting Closing
Personal information inconsistent with information already on file at financial institution or creditor.	Because the nature of the mortgage industry, we normally do not receive multiple applications for individuals. Simply receiving one would be a red flag.	Servicer
Person opening account or customer unable to correctly answer challenge questions.	Mortgage lenders Normally complete face to face or in person applications, and do not open multiple accounts. The “password challenge” protocol is normally designed for online Password protected accounts.	Servicers Home equity lenders
Shortly after change of address, creditor receiving request for additional users of account.	Unless the account is a home equity line of credit, already being serviced, there’s little likelihood of a mortgage originator adding additional borrowers or “users” to an application	Servicers Home equity lenders
Most of available credit used for cash advances, jewelry or electronics, plus customer fails to make first payment.	The risk of this type of applicant is addressed in credit scoring but not for particular accounts. We address high credit limits relative to credit balances, the number of payments on time, the newness of accounts. Only home equity lending can see utilization usage of credit patterns.	Home Equity Lender
Drastic change in payment patterns, use of available credit or spending patterns.	Any pattern of late payment would be a red flag for a loan servicing function.	Servicing
An account that has been inactive for a lengthy time suddenly exhibiting unusual activity.	For any account which is a line of credit, said an unusual activity is a red flag.	Servicing
Mail sent to customer repeatedly returned as undeliverable despite ongoing transactions on active account.	Return mail is a particularly troubling red flag. Normally any mail is delivered to the address that the customer lists on the application. Mail would be returned long before the application was consummated	Origination Processing Servicing
Financial institution or creditor notified that customer is not receiving paper account statements.	This could be an early sign of “house stealing”.	Servicing
Financial institution or creditor notified of unauthorized charges or transactions on customer's account.	For any revolving line of credit, construction loan, home equity lines of credit, is the potential for unauthorized credit line advances.	Construction Administration Servicing
Financial institution or creditor notified that it has opened a fraudulent account for a person engaged in identity theft.	Once the account is in place, and is reported to the credit bureaus, borrowers who have been victims of identity theft and fraud will be able to locate accounts opened as a result of this activity.	Servicing

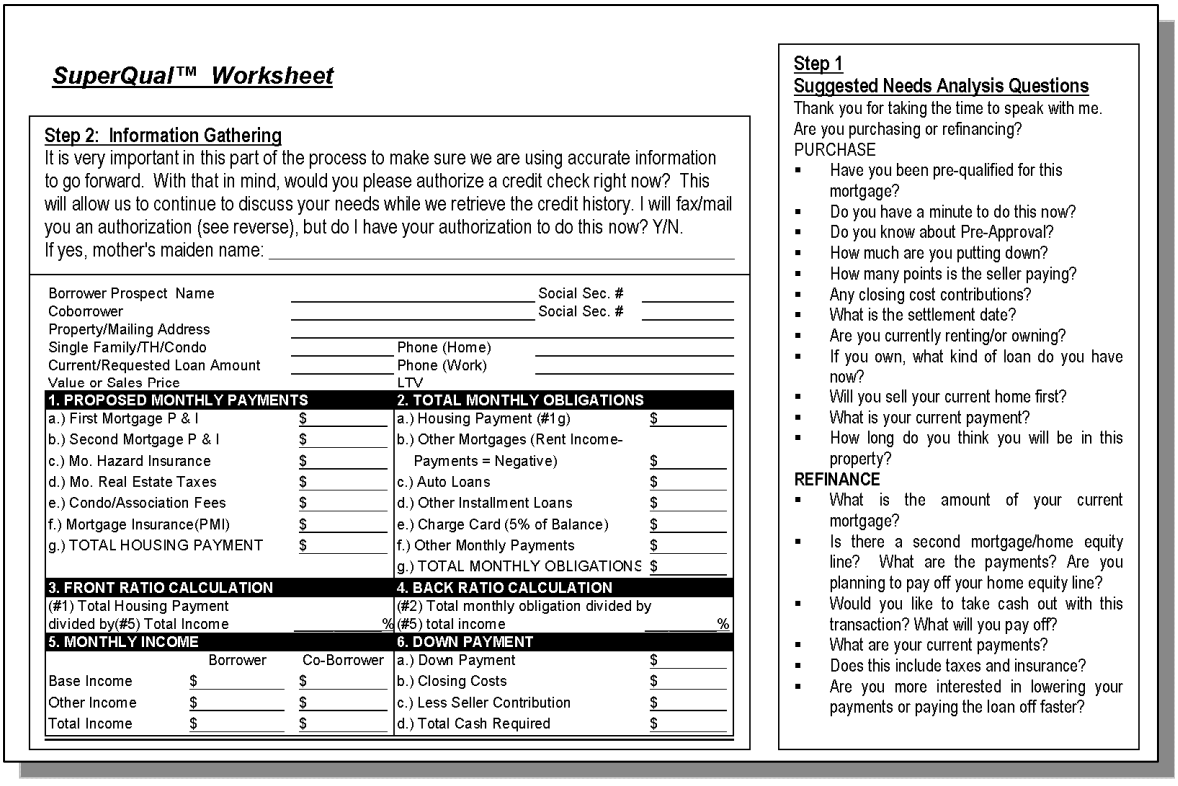
Originator's Role in Red Flag Actions

The loan originator is the first customer contact. The loan originator acts as a field underwriter, anticipating problems on the case file and providing solutions. At the initial Pre-Qualification one of the first tasks loan officer will address is how much the borrower can afford. From this point the loan originator will proceed to request authorization to order credit report and the remaining income, asset and transaction supporting documentation.

Pre-Qualification and Qualification

In a Pre-Qualification, the loan originator will not necessarily accept a formal loan application to be setup. The loan originator is simply trying to identify whether the applicant is eligible for financing. In this process the customer may authorize the loan originator to investigate credit history. It is at this time that the loan originator may become aware that the applicant is a victim or potential perpetrator of identity theft.

In this circumstance Company Name requires that loan originator keep a record of the qualification calculations as evidence that all debts reviewed on the credit report have been acknowledged by the borrower. In addition, in compliance with the equal credit opportunity act, the loan originator may send the borrower a copy of the adverse information notification and credit score disclosure.



SuperQual™ Worksheet

Step 2: Information Gathering

It is very important in this part of the process to make sure we are using accurate information to go forward. With that in mind, would you please authorize a credit check right now? This will allow us to continue to discuss your needs while we retrieve the credit history. I will fax/mail you an authorization (see reverse), but do I have your authorization to do this now? Y/N.
If yes, mother's maiden name: _____

Borrower Prospect Name		Social Sec. #	
Coborrower		Social Sec. #	
Property/Mailing Address			
Single Family/TH/Condo		Phone (Home)	
Current/Requested Loan Amount		Phone (Work)	
Value or Sales Price		LTV	

1. PROPOSED MONTHLY PAYMENTS		2. TOTAL MONTHLY OBLIGATIONS	
a.) First Mortgage P & I	$	a.) Housing Payment (#1g)	$
b.) Second Mortgage P & I	$	b.) Other Mortgages (Rent Income- Payments = Negative)	$
c.) Mo. Hazard Insurance	$	c.) Auto Loans	$
d.) Mo. Real Estate Taxes	$	d.) Other Installment Loans	$
e.) Condo/Association Fees	$	e.) Charge Card (5% of Balance)	$
f.) Mortgage Insurance(PMI)	$	f.) Other Monthly Payments	$
g.) TOTAL HOUSING PAYMENT	$	g.) TOTAL MONTHLY OBLIGATIONS	$
3. FRONT RATIO CALCULATION		**4. BACK RATIO CALCULATION**	
(#1) Total Housing Payment divided by(#5) Total Income	%	(#2) Total monthly obligation divided by (#5) total income	%

5. MONTHLY INCOME	Borrower	Co-Borrower	6. DOWN PAYMENT	
Base Income	$	$	a.) Down Payment	$
Other Income	$	$	b.) Closing Costs	$
Total Income	$	$	c.) Less Seller Contribution	$
			d.) Total Cash Required	$

Step 1
Suggested Needs Analysis Questions

Thank you for taking the time to speak with me. Are you purchasing or refinancing?

PURCHASE

- Have you been pre-qualified for this mortgage?
- Do you have a minute to do this now?
- Do you know about Pre-Approval?
- How much are you putting down?
- How many points is the seller paying?
- Any closing cost contributions?
- What is the settlement date?
- Are you currently renting/or owning?
- If you own, what kind of loan do you have now?
- Will you sell your current home first?
- What is your current payment?
- How long do you think you will be in this property?

REFINANCE

- What is the amount of your current mortgage?
- Is there a second mortgage/home equity line? What are the payments? Are you planning to pay off your home equity line?
- Would you like to take cash out with this transaction? What will you pay off?
- What are your current payments?
- Does this include taxes and insurance?
- Are you more interested in lowering your payments or paying the loan off faster?

Origination Review – Borrower Identity

ORIGINATION QUALITY CONTROL, RED FLAG AND FRAUD REVIEW Checklist

Originator Notes Regarding Credit/Personal Situations

CREDIT / CREDIT REPORTS

- No credit (possible use of alias)
- High income borrower with little or no cash (undisclosed liabilities)
- Variance in employment or residence data from other sources
- Recent inquiries from other mortgage lenders
- Invalid social security number
- AKA or DBA indicated
- Round dollar amounts (especially on interest-bearing accounts)
- Borrower cannot be reached at place of business
- High income borrower with no "prestige" credit cards
- Credit report includes a fraud, credit freeze, address discrepancy or active duty alert h a consumer report.
- A recent and significant increase in the volume of inquiries;
- An unusual number of recently established credit relationships;
- A material change in the use of credit, especially with respect to recently established credit relationships; or
- An account that was closed for cause or identified for abuse of account privileges by a financial institution or creditor.
- The Social Security Number (SSN) has not been issued, or is listed on the Social Security Administration's Death Master File.
- There is a lack of correlation between the SSN range and date of birth.
- The address on an application is fictitious, a mail drop, or a prison; or
- The phone number is invalid, or is associated with a pager or answering service.
- Notice from Customers, Victims of Identity Theft, Law Enforcement Authorities, or Other Persons Regarding Possible Identity Theft

Section III & IV - Borrower Information & Employment

- ❑ Borrower's Complete Name, Jr., Sr. ID Variance?
- ❑ Social Security Number Match
- ❑ 30 Days' Pay stubs
- ❑ 2 Years W-2's
- ❑ Self Employed at least 2 years?
- ❑ Two Years 1040's/1120/1065
- ❑ Non-Schedule C business credit report necessary?
- ❑ Any Job Gaps/Different Employers? get letter
- ❑ Have they moved recently?
- ❑ Recently Married? What is maiden name?
- ❑ Recently married with Older Kids – do you need a divorce decree or separation agreement – include child support

1. Credit and Personal Information –
Insert In Front of Credit Report

Red Flag Review Form
Page 1 - Credit and Personal Financial Information
Revised 10/6/2008

Originator Review – Income and Employment Documentation

ORIGINATION QUALITY CONTROL, RED FLAG AND FRAUD REVIEW Checklist

Originator Notes Regarding Income/Employment Situations

EMPLOYMENT / EMPLOYMENT VERIFICATION

- Employee is paid monthly
- No prior year earnings on VOE
- Gross earnings per VOE for commission-only employees should not be used (see IRS Form 1040 Schedule C)
- Borrower is a business professional (may be self-employed)
- Answering machine or service at place of business (may be self-employed)
- Prior employer "out of business"
- Seller has same address as employer
- Employer signs VOE prior to date it was mailed by the lender
- Borrower uses employer's letterhead for letters of explanation
- Employment verified by someone other than personnel department
- Pay stubs are not preprinted for a large employer
- Pay stubs are handwritten for a large employer
- Current and prior employment overlap
- Date of hire is weekend or holiday
- Income is primarily commissions or consulting fees (Self-employment)
- Employer uses mail drop or post office box for conducting business
- Change in profession from previous to current employer
- Borrower is a professional employee not registered/licensed (doctor, lawyer, architect, real estate broker, etc)
- Illegible employer signature with no further identification
- Inappropriate verification source (secretary, relative, etc.)
- Document is not folded (never mailed)
- Evidence of ink eradicator (whiteout) or other alterations
- Verification "returned to sender" for any reason
- Inappropriate salary with respect to amount of loan

SELF EMPLOYED

- (Some "red flags" are indicators that someone may be self employed, these are important if a borrower has not revealed themselves to be self employed)
- Business entity not registered or in good standing with the applicable regulatory agencies.
- Address and/or profession does not agree with other information submitted on the loan application
- Tax computation does not agree with tax tables
- No estimated tax payments made by self-employed borrower (Schedule SE required)
- No FICA taxes paid by self-employed borrower (Schedule SE required)
- Self employment income shown as wages and salaries
- Income or deductions in even dollar amounts
- High bracket taxpayer with few or no deductions or tax shelters
- High bracket taxpayer does not use a professional tax preparer.
- Paid preparer signs taxpayer's copy
- Paid preparer hand-writes tax return

2. Income Employment Information -
Place on top of Income Documentation

Red Flag Review Form
Page 2 – Income and Housing Expense Information
Revised 10/6/2008

ORIGINATION QUALITY CONTROL, RED FLAG AND FRAUD REVIEW Checklist

TAX RETURNS

- Schedule A – Real estate taxes paid but no property owned
- Schedule A – No interest expense paid when borrower shows ownership of property (or vice versa)
- Schedule A – Employee who deducts business expenses (check against Form 2106)
- Schedule B – Amount or source of income doesn't agree with information submitted on loan application
- Schedule B – No dividends earned on stock owned (may be closely held)
- Schedule B – Borrower with substantial cash in bank shows little or no related interest income
- Schedule C – Gross income does not agree with total income per Form 1099
- Schedule C – Borrower shows interest expense but no related loan (business loans with personal liability)
- Schedule C – Borrower takes a depreciation deduction for real estate no disclosed (or vice versa)
- Schedule C – No IRA or Keogh deduction
- Schedule C – No salaries paid on non-service companies
- Schedule C – No "cost of goods sole" on retail or similar operations
- Schedule C – No schedule SE filed (computation of self-employed tax)
- Schedule E – Net income from rents plus depreciation does not equal cash flow as submitted by borrower.
- Schedule E – Additional properties listed by not on loan application
- Schedule E – Borrower shows partnership income (may be liable as a general partner for partnership's debts)
- Form W-2 – Invalid employer identification number
- Form W2 – FICA and local taxes withheld (where applicable) exceed ceilings
- Form W2 – Copy submitted is not "Employee's Copy" (Copy C)
- Form W2 – Large employer has handwritten or typed W-2

Section V - Income & Housing Expense

- ❑ Examine Pay stub
- ❑ Salary evident from pay stub?
- ❑ Yr. to Date Higher/Lower than base salary? - Document/Explain
- ❑ Deductions - Any Loans? Shown on Credit Report? if not request rating
- ❑ Retirement? - Get Statement
- ❑ Bonus/Overtime/Commissions 25%
- ❑ Job Gaps
- ❑ Decrease in rate? Explain
- ❑ Complex History/Many Job Changes/Change in Company Name? Explain
- ❑ Rent amount? - Get Landlord Name & Number
- ❑ Mortgage Amount - Shown on Credit Report? - if no, need 12 months checks

Red Flag Review Form
Page 3 – Income and Housing Expense Information
Revised 10/6/2008

Originator Review – Asset Documentation

ORIGINATION QUALITY CONTROL, RED FLAG AND FRAUD REVIEW Checklist

Originator Notes Regarding Asset Situations

VERIFICATION OF ASSETS /DEPOSIT / BANK STATEMENT

- Regular deposits (payroll) significantly at odds with reported income
- Earnest Money Deposit not debited to checking account
- NSF items require explanation.
- Large withdrawals may indicate undisclosed financial obligations or investments
- Lower income borrower with recent large accumulation of cash
- Bank account is not in borrower's name (business entity, trust funds, etc.)
- Evidence of ink eradicator (whiteout) or other alterations
- Verification "returned to sender" for any reason
- High income borrower with little or no cash (undisclosed liabilities)
- IRA is shown as a liquid asset or a source of down payment
- Non-depository "depository" (escrow trust account, title company, etc.)
- Credit union for small employer
- Borrower's funds are security for a loan
- Illegible bank employee signature with no further identification
- Source of funds consist of (unverified) note, equity exchange or sale of residence
- Cash in bank not sufficient to close escrow
- New bank account
- Gift letters must be carefully reviewed (canceled checks, bank statements)
- Borrower has no bank accounts (doesn't believe in banks)
- Document is not folded (never mailed)
- Young borrower with large accumulation of unsubstantiated assets
- Young borrowers with substantial cash in bank

Section VI - Assets & Liabilities

- ❑ Copy of Earnest Money Check - Agrees with Contract?
- ❑ Review Bank Statements – Major Increases or Decreases?
- ❑ Funds for Closing Evident? - When received & What
- ❑ Any large withdrawals, deposits? - Explain & Document
- ❑ Net Worth Business? Self-employed P&L
- ❑ Cars owned free & clear? Titles?
- ❑ Other assets? Anything? Anything?
- ❑ Liabilities Reported not reported or verified?
- ❑ Credit explanations needed?
- ❑ Proof of Payoff?
- ❑ Real Estate Schedule - Rental Property on Tax Returns?
- ❑ Leases for Rentals

3. Asset Documentation –

Place in front of Asset Verification in file

Red Flag Review Form
Page 4 – Asset Information
Revised 10/6/2006

Originator Review – Property Information

ORIGINATION QUALITY CONTROL, RED FLAG AND FRAUD REVIEW
Checklist

Originator Notes Regarding Property and Disclosures

APPRAISAL

- Ordered by a party to the transaction (seller, buyer, broker, etc.)
- Comps are not verified as recorded or submitted by potentially biased party (seller, real estate broker)
- Tenant shown to be contact on owner-occupied property
- Income approach not used on tenant-occupied SFR
- Appraiser uses FNMA number as sole credential (discontinued program)
- Market approach substantially exceeds replacement cost approach
- "For Sale" sign on the photos of the subject (in refinance loans)
- HUD-1 or grant deed on original purchase is less than two years old (for refinance loans)

Section I&II - Property Information Read The Sales Contract
Check the Sales Contract for

- ❑ Loan Amount/Down Payment Correct?(can you do the loan?)
- ❑ Settlement Date Reasonable?
- ❑ Contract Signed by all?
- ❑ Seller Contributions w/in Guidelines
- ❑ No Decorator/Repair Allowance
- ❑ Interest Rate/Points Available

Audit Property for

- ❑ Condo/PUD/Coop/ -is it on list? Make Sure you get PUD/Condo Docs/ Check Fee in PITI
- ❑ Property Info **If Refinance** Check Deed for Titling
- ❑ Legal Description
- ❑ Ask for Survey
- ❑ Construction Permanent - Land Cost/Value – Construction Costs Documented?
- ❑ 2nd Mortgage to be subordinated?
- ❑ New Home – Request Future addendums Changing Sales Price
- ❑ Investment Property – is current home worth more than proposed property?
- ❑ Listing Printout
- ❑ Is the Property Serviced by Well/Septic (Rural)
- ❑ Private Road (Not publicly Maintained - Rural) Need a Road Maintenance Agreement

4. Property/Contract Information –
Insert before sales contract/appraisal

Red Flag Review Form
Page 5 – Property Information
Revised 10/6/2008

Loan Processing Red Flag Review

Upon completion of the loan origination file setup a file is passed to loan processing for vendor orders, additional documentation requests, and underwriting file preparation. It is that this stage that items that might not have been immediately apparent to the loan originator reveal themselves to the processor.

Loan processors must be particularly vigilant in reviewing discrepancies, has information which is revealed at this stage of the loan process is normally a more subtle in its variances.

For this process we provide loan processor setup checklist. This is part of the standard quality control review process for loan processing intake and loan processing submission. Red flag items have been added as appropriate to the stage.

Processor/Underwriter Red Flag - Application Review

Pre-Underwriting Submission Checklist

	GENERAL ITEMS
☐	Lock Still Valid?
☐	LTV within Guidelines?
☐	Within Maximum/Minimum Loan Amount?
☐	Fee sheet completed?
☐	Signed lock-in, financing, broker agreement in file?
☐	Assignment letter to investor?
☐	All borrowers occupy
☐	Non-Occupant Co-borrower Guidelines Met
☐	PMI Required?
☐	Coverage Correct on Certificate?
☐	Red Flag - No Returned Mail in File
☐	Copy package for PMI? Correct number of packages for Investor?
	Loan Analysis - 1008, 92900WS, 6393
☐	Borrower information correct - same on initial & final 1003?
☐	PITI correct and same as 1003 and addendum?
☐	If ARM or buy down, indicate qualify rate?
☐	ARM Disclosure if ARM?
☐	Program Specifications - Ratios different for buy downs?
☐	All debts as listed on credit report and verifications?
☐	1008/2900 WS ratios in line with loan program?
☐	FHA/VA calvrs #'s
☐	Maximum Number of Properties Financed
☐	Is 2nd Allowed Under Program
☐	Is CLTV in Guidelines
☐	Are terms of 2nd Acceptable
	FINAL TYPED LOAN APPLICATION (1003/URLA)
☐	Match pay stubs?
☐	W-2
☐	RED FLAG - Photo ID
☐	Credit Report
☐	Initial 1003 - Any Alterations RED FLAG
☐	2 years employment/residency? RED FLAG
☐	Assets/liabilities agree with initial 1003 and loan analysis - undisclosed debts?
☐	home, time share or land owned free and clear - do you have evidence - have you counted taxes, insurance, condo, hoa, management fees as debts?
☐	Government monitoring completed initial/final 1003?
☐	Immigration, social security card or green card if resident alien? RED FLAG
☐	Property Address, Legal Agree with Title, Sales Contract?

Pre-Underwriting Checklist
page 1 of 5
10/6/2008

Processor/Underwriter Red Flag Review – Credit Report, Employment and Income Verification

Pre-Underwriting Submission Checklist

	Credit Report - Liabilities
☐	ss#s names, match original/typed 1003 and photo id (FHA only)
☐	2 years residency verified with 12 month current payment history
☐	If using vom/vor/vol or paid off mortgage reference - list "See Independent Verification" on 1003.
☐	if line of credit subordinated, need full terms, count maximum line and payment
☐	12 months reviewed on all mortgage/installment loans-balances w/in 90 days
☐	12 months cancelled checks on co-signed loans-balances within 90 days
☐	all "creditor declines" or "written verification to update" are verified - Red Flag
☐	satisfactory explanation with documentation for all derogatory credit
☐	open judgments/collections/past due/charge offs - must clear PTC "Public Records Checked"
☐	satisfactory explanation for credit inquiries with new accounts verified - Red Flag
☐	debts on credit report match original/typed 1003/loan analysis – if not explanation for undisclosed debts
☐	alimony/child support/child care counted as debt or reduction in income as documented by separation agreement/divorce decree
☐	Dates agree with Application Date?
☐	Red Flag - Fraud, active duty alert, credit freeze, notice of address discrepancy, pattern of activity that is inconsistent, with the history and usual pattern of activity of an applicant
☐	All Credit Reports ordered in file?
☐	WRITTEN PAYOFF STATEMENT accurate/current written payoff statement for all loans. Payoff may be updated verbally with processor cert. however the initial written payoff cannot be more than 90 days from UW
	EMPLOYMENT/INCOME
☐	2 year history - explain/document gaps > 3 weeks
☐	Income inconsistent? Provide satisfactory documentation from employer on letterhead
☐	Income Computation Memo - Explain how income derived
☐	Overtime/bonus/commission - 25% of total earnings? Need 2 years complete tax returns and continuance verified
☐	Un-reimbursed business expenses? Calculated and income reduced
☐	Any loan/unusual deduction on pay stub?
	FULL DOCUMENTATION
☐	Fully completed, signed, dated V.O.E. all information is completed, initialed
☐	Current YTD pay stub - FHA no older than 30 days at time of approval
☐	W-2's for past two years
	ALTERNATIVE DOCUMENTATION
☐	Verbal verification certification signed by processor
☐	current year to date pay stubs to cover 30 day period (bi-weekly employees = 3 pay stubs)
☐	W-2's for past two years
	SELF EMPLOYED
☐	Two years personal/corporate/partnership tax returns
☐	K-1's, with all schedules and signed by borrowers
☐	IRS form 4506/1820 signed
☐	Current year to date profit and loss, balance sheet signed by preparer
☐	FNMA 1084 (self employment analysis) completed
	RETIREMENT VA DISABILITY PENSION CHILDS SUPPORT ALIMONY, NOTE INCOME
☐	Two years' 1099's
☐	Evidence of receipt for last 12 months
☐	Income going to continue for 3 years for FNMA/FHLMC - 5 years FHA/VA
☐	Award letter
☐	Divorce decree, separation agreement
	DIVIDEND/INTEREST
☐	Two years tax returns
☐	YTD dividend/interest earnings from bank
☐	Money needed for closing? Deduct from liquid assets
	LEASE/RENTAL INCOME
☐	Two years tax returns
☐	Current leases required on all properties - tenant letters if month to month
☐	Expenses counted on Schedule E
☐	real estate owned schedule
☐	FHA/VA Streamline - income verification not necessary as long as borrowers remain listed as on original loan
☐	Property Management Letter if professionally managed

Pre-Underwriting Checklist
page 2 of 5
10/6/2008

Processor/Underwriter Red Flag Review – Asset Documentation

Pre-Underwriting Submission Checklist

	ASSETS
☐	Are adequate funds for closing/reserves verified
☐	Any large deposits explained/documented
☐	Gift funds adequately documented? (Transfer, Receipt, Donor's Ability -Source)
☐	Completed, signed gift letter
☐	Transfer of funds
☐	Receipt of funds
☐	Updated bank balance, ATM RECEIPT NOT ACCEPTABLE
☐	2 (or 3) consecutive current bank statements for ALT DOC must be certified true copies (original on va loans)
☐	Verification of Deposit with 2 month average balance? (If not then Bank Statements?)
☐	Two months current bank statements?
☐	Does borrower have own 5% (FNMA/FHLMC)
☐	Earnest money deposit adequately verified
☐	All accounts are updated stock/bonds/IRA/CD/401k/thrift savings plan
☐	3 consecutive current statements/or most current quarterly statement
☐	IRA/401(k) penalty calculated? Sufficient funds remain to cover all costs?
☐	Is liquidation properly documented
☐	Properly document whether repayment IS or IS NOT required
☐	One month bank statement dated within 45 days for FHA/VA streamline

Pre-Underwriting Checklist
page 3 of 5
10/6/2008

Processor/Underwriter Red Flag Review – Transaction

Pre-Underwriting Submission Checklist

	PROPERTY
☐	Is property complete?
☐	Final Inspection Ordered?
☐	Recertification of value (over 4 months?)
☐	Check Dates of Transfer on Appraisal/Title Report 0 < 12 months
☐	Are repairs required?
☐	Private road maintenance agreement?
☐	Flood insurance?
☐	Well/septic?
☐	FHA/VA project approval
☐	FNMA/FHLMC warranty for condo/pud
☐	Condo/HOA/PUD questionnaire or association management letter
☐	Certificate of Insurance - Condo/PUD
☐	Investment property - completed operating income statement and rent comparable schedule (FNMA/FHLMC)
☐	Make sure with realtor/builder no changes Final Sales Price made
☐	Sales Contract and all addenda to sales contract - signed
☐	Contract - check seller paid items; closing costs, points, allowances conform to program guidelines
☐	Relocation Agreement – Terms Highlighted
☐	Contract - all contingencies satisfied and removed
	Appraisal
☐	All blanks filled in and signed?
☐	Appraisers conclusions and market value estimates supported ?
☐	Are comparable sales similar in design and appeal?
☐	Gross adjustments don't exceed 25% , net adjustments don't exceed 10%?
☐	Legal/address confirm with other property information?
☐	Is appraisal date before application date?
☐	Does the photographs have a for sale sign on refinance?
☐	Twelve months listing history (FHA) 24 months listing history
☐	Sellers name same on appraisal as on title?
	DISCLOSURES
☐	Initial GFE and TIL within 3 days of loan application
☐	Redisclosed TIL/GFE and Financing Agreement if initial amount, type of financing changed
☐	Red Flag - Patriot ACT - Photo ID Match
☐	ECOA Disclosure
☐	Transfer of Servicing disclosure
☐	Borrower certification and authorization
☐	Broker Agreement, Financing Agreement
☐	Blanket Disclosure - Occupancy statement
☐	ARM/Balloon/Prepayment Penalty and Program disclosures
	Refinance
☐	IS LTV acceptable
☐	Cash Out Purpose
☐	Is loan amount, dollar amount of cash out allowed
☐	Is seasoning met
☐	Tangible Net benefit Calculation - Purpose of Refinance statement
☐	Appraisal not needed for FHA Streamline VA Fasttrack (unless financing closing costs above original loan amount)
☐	Deed/Title matches borrowers

Pre-Underwriting Checklist
page 4 of 5
10/6/2008

Verbal Verification of Employment

The purpose of the verbal employment verification is to confirm the borrower's employment data in the event written employment verification was not obtained - such as is the case when utilizing alternative documentation. This is a red flag review to determine whether the applicant's documentation are matched with an actual employer. In addition, it is used to confirm that the borrower's employment status hasn't changed since the date of the loan approval.

Procedure

Step 1 Form	Prepare the employment verification form by printing the Verbal VOE document. Have the application form available in the event you need to change or confirm information or otherwise identify the applicant.
Step 2 Independent Verification	Independently verify the name, address and telephone number of the employer. Identify the information source utilized, i.e.; 411, yellow pages, internet, etc.
Step 3 Attempt Verification	Contact the employer through the number verified. State the purpose of the call to whoever answers the telephone and request to speak with the individual responsible for verifying employment. Record the responses when they involve re-directing the call to another number or office.
Step 4 Interview	When the correct authority is contacted, note their direct dial number, their name and title. Request the information that needs to be verified. Often the information cannot be volunteered, the verifier must provide the information the borrower supplied and have the authority confirm it. If they cannot give exact information, record what the authority does provide - such as "over 5 years", etc.
Step 5 Findings	Record the information and sign the form. If there is an adverse finding in the information, or if there are questions as to the authenticity of the verifier, report these incidents to management - do not attempt to confront the borrower regarding this.

Probability of Continued Employment is the most critical question to be answered. Often the authority doesn't volunteer this information. If this is the case ask if there is any reason to question continued employment. If the employer can state that there is no reason to question, simply record "no reason to question".

In addition, the requestor may find the authority intractable as to providing information. In this case, call directly to the individual's office and verify through an administrative personnel staff member the borrower's employment.

«lender_name»

«lender_address_1»
«lender_address_2»
«lender_phone»

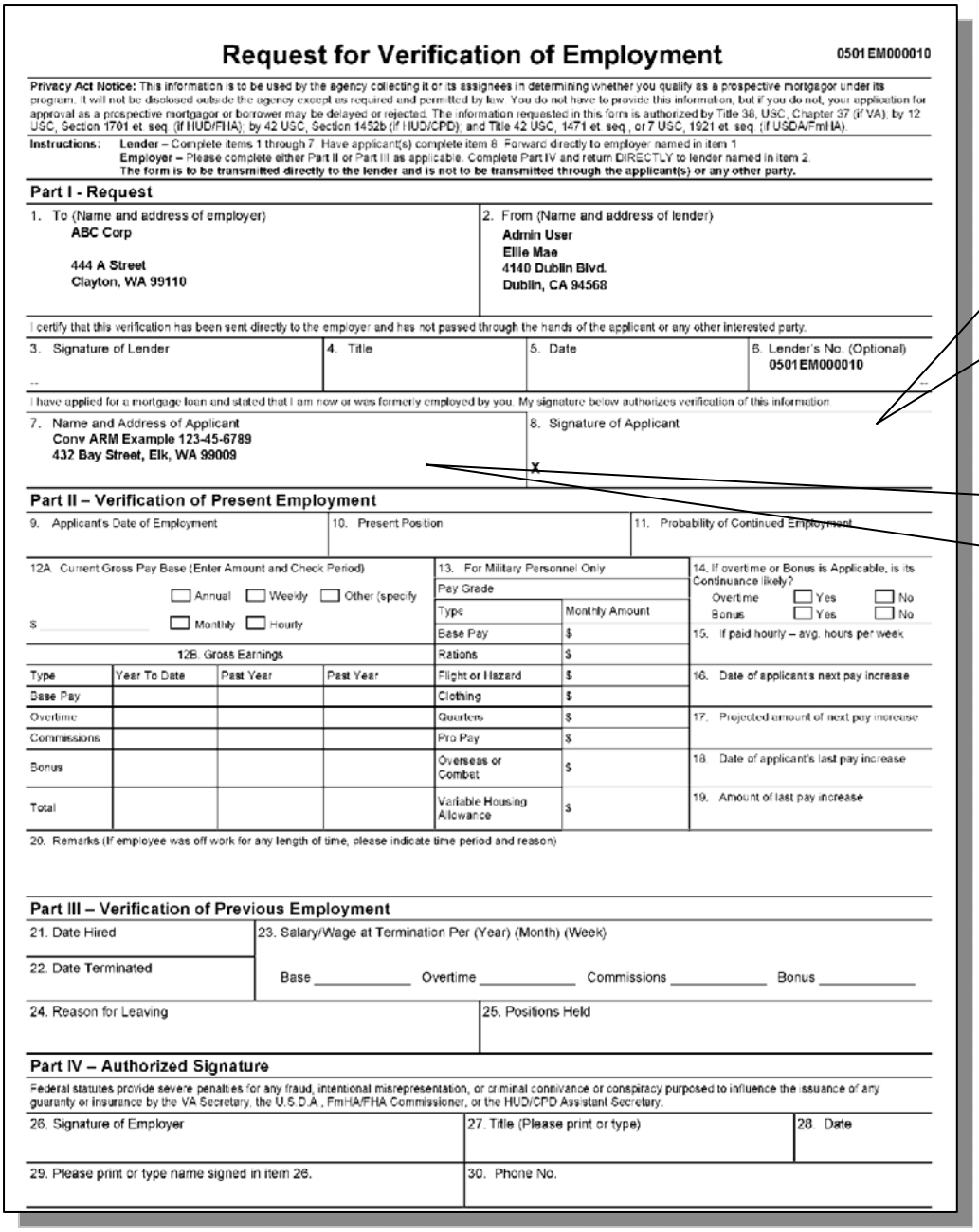
Verbal Verification of Employment

Borrower:	«bor_first_name» «bor_last_name»
Property Address:	«subject_address» «subject_city», «subject_state» «subject_zip»
Employee ID/SS#	«borrower_ssn»
Employer:	
Employer Phone:	«bor_bus_phone»
Directory Assistance:	
Person Contacted:	
Title:	
Date of Employment:	
Position:	
Employment Status (full/pt)	
Probability of Continued Employment	
Eligible for Bonus/Overtime/Incentive	
Current Salary	
Per (year/month/bi-monthly/bi-weekly/hrly)	
If Income was not verified state reason	

I hereby certify that this information was personally verified by me and is true and correct to the best of my knowledge and belief.

By:_____
«lender_name»

Truncating Social Security Numbers on Requests



Request for Verification of Employment

0501EM000010

Privacy Act Notice: This information is to be used by the agency collecting it or its assignees in determining whether you qualify as a prospective mortgagor under its program. It will not be disclosed outside the agency except as required and permitted by law. You do not have to provide this information, but if you do not, your application for approval as a prospective mortgagor or borrower may be delayed or rejected. The information requested in this form is authorized by Title 38, USC, Chapter 37 (if VA); by 12 USC, Section 1701 et seq. (if HUD/FHA); by 42 USC, Section 1452b (if HUD/CPD); and Title 42 USC, 1471 et seq., or 7 USC, 1921 et seq. (if USDA/FmHA).

Instructions: **Lender** – Complete items 1 through 7. Have applicant(s) complete item 8. Forward directly to employer named in item 1.
Employer – Please complete either Part II or Part III as applicable. Complete Part IV and return DIRECTLY to lender named in item 2.
The form is to be transmitted directly to the lender and is not to be transmitted through the applicant(s) or any other party.

Part I - Request

1. To (Name and address of employer)
ABC Corp
444 A Street
Clayton, WA 99110

2. From (Name and address of lender)
Admin User
Ellie Mae
4140 Dublin Blvd.
Dublin, CA 94568

I certify that this verification has been sent directly to the employer and has not passed through the hands of the applicant or any other interested party.

3. Signature of Lender	4. Title	5. Date	6. Lender's No. (Optional)
--			**0501EM000010**

I have applied for a mortgage loan and stated that I am now or was formerly employed by you. My signature below authorizes verification of this information.

7. Name and Address of Applicant	8. Signature of Applicant
Conv ARM Example 123-45-6789 **432 Bay Street, Elk, WA 99009**	**X**

Part II – Verification of Present Employment

9. Applicant's Date of Employment	10. Present Position	11. Probability of Continued Employment

12A. Current Gross Pay Base (Enter Amount and Check Period)	13. For Military Personnel Only		14. If overtime or Bonus is Applicable, is its Continuance likely?
☐ Annual ☐ Weekly ☐ Other (specify	Pay Grade		Overtime ☐ Yes ☐ No
$ ☐ Monthly ☐ Hourly	Type	Monthly Amount	Bonus ☐ Yes ☐ No
	Base Pay	$	15. If paid hourly – avg. hours per week

12B. Gross Earnings						
Type	Year To Date	Past Year	Past Year	Flight or Hazard	$	16. Date of applicant's next pay increase
Base Pay				Clothing	$	
Overtime				Quarters	$	17. Projected amount of next pay increase
Commissions				Pro Pay	$	
Bonus				Overseas or Combat	$	18. Date of applicant's last pay increase
Total				Variable Housing Allowance	$	19. Amount of last pay increase

20. Remarks (If employee was off work for any length of time, please indicate time period and reason)

Part III – Verification of Previous Employment

21. Date Hired	23. Salary/Wage at Termination Per (Year) (Month) (Week)
22. Date Terminated	Base _____ Overtime _____ Commissions _____ Bonus _____
24. Reason for Leaving	25. Positions Held

Part IV – Authorized Signature

Federal statutes provide severe penalties for any fraud, intentional misrepresentation, or criminal connivance or conspiracy purposed to influence the issuance of any guaranty or insurance by the VA Secretary, the U.S.D.A., FmHA/FHA Commissioner, or the HUD/CPD Assistant Secretary.

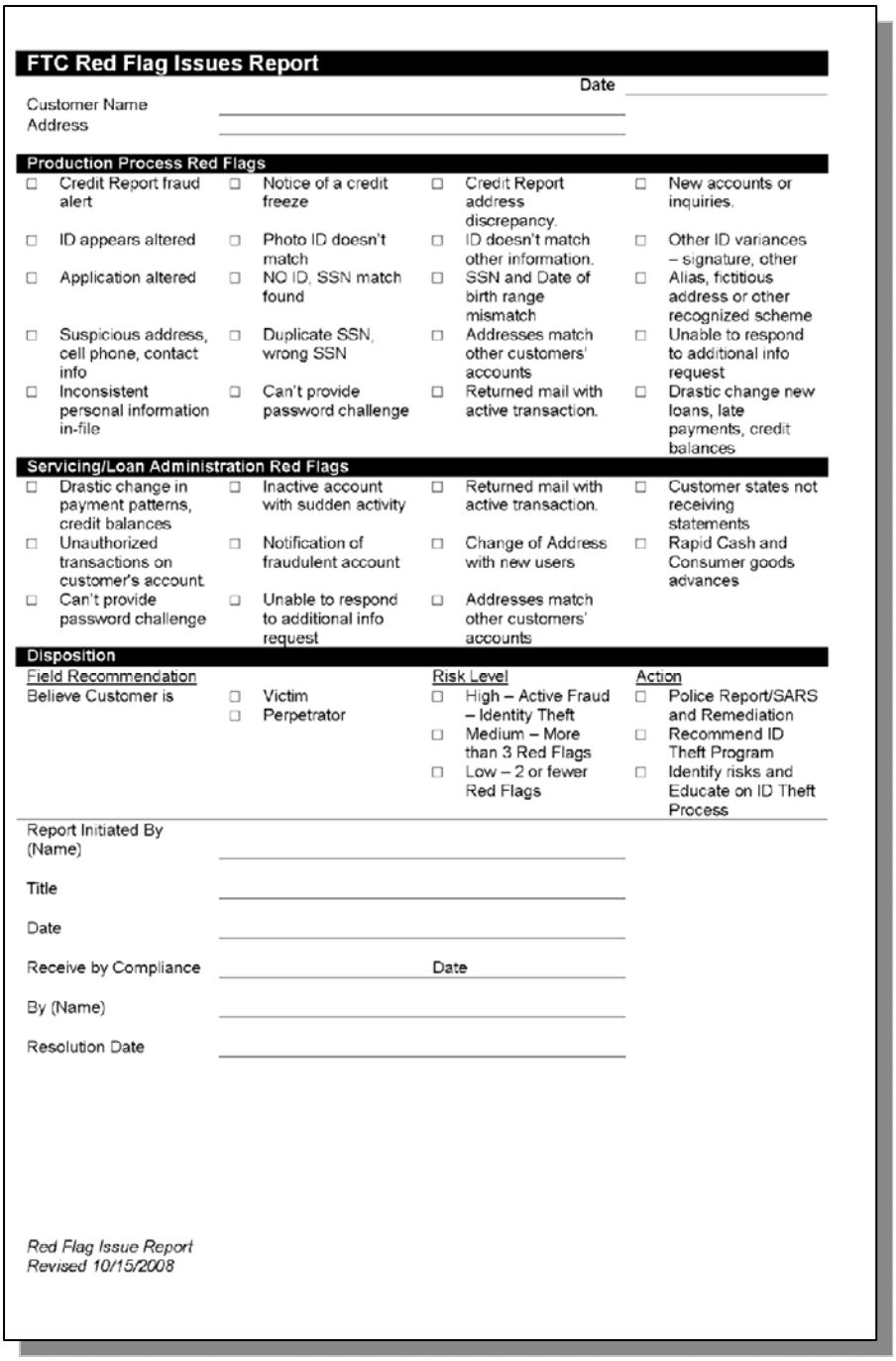
26. Signature of Employer	27. Title (Please print or type)	28. Date
29. Please print or type name signed in item 26.	30. Phone No.	

Attached Signature Requests: The blanket credit authorization may have a social security number on it. Do not send it without eliminating the first 5 digits.

Truncating Identification Information: Do NOT include personal identifying information on the request for verification – signature authorization should be sufficient.

Section 6 – Red Flag Discovery and Process

If a staff member discovers any red flag in the process of working with a borrower, he or she must immediately complete a Red Flag Issue Report Form and forward it to the designated manager, quality control or compliance staff member.



FTC Red Flag Issues Report

Date _____

Customer Name _____
Address _____

Production Process Red Flags

☐ Credit Report fraud alert	☐ Notice of a credit freeze	☐ Credit Report address discrepancy.	☐ New accounts or inquiries.
☐ ID appears altered	☐ Photo ID doesn't match	☐ ID doesn't match other information.	☐ Other ID variances – signature, other
☐ Application altered	☐ NO ID, SSN match found	☐ SSN and Date of birth range mismatch	☐ Alias, fictitious address or other recognized scheme
☐ Suspicious address, cell phone, contact info	☐ Duplicate SSN, wrong SSN	☐ Addresses match other customers' accounts	☐ Unable to respond to additional info request
☐ Inconsistent personal information in-file	☐ Can't provide password challenge	☐ Returned mail with active transaction.	☐ Drastic change new loans, late payments, credit balances

Servicing/Loan Administration Red Flags

☐ Drastic change in payment patterns, credit balances	☐ Inactive account with sudden activity	☐ Returned mail with active transaction.	☐ Customer states not receiving statements
☐ Unauthorized transactions on customer's account	☐ Notification of fraudulent account	☐ Change of Address with new users	☐ Rapid Cash and Consumer goods advances
☐ Can't provide password challenge	☐ Unable to respond to additional info request	☐ Addresses match other customers' accounts	

Disposition

Field Recommendation		Risk Level	Action
Believe Customer is	☐ Victim ☐ Perpetrator	☐ High – Active Fraud – Identity Theft ☐ Medium – More than 3 Red Flags ☐ Low – 2 or fewer Red Flags	☐ Police Report/SARS and Remediation ☐ Recommend ID Theft Program ☐ Identify risks and Educate on ID Theft Process

Report Initiated By (Name) _____

Title _____

Date _____

Receive by Compliance _____ Date _____

By (Name) _____

Resolution Date _____

Red Flag Issue Report
Revised 10/15/2008

Working with Borrowers -Counseling the Public

In our role as mortgage lenders we represent a human face to what is often a monolithic credit industry. Our customer interaction, our relationships with our referral sources, and our interaction with credit industry vendors gives us a unique ability to educate and to intervene.

Company Name will support the use of seminars and educational material for the public in general. Individual consumers will be instructed as to the best practices for maintaining privacy of their personal financial information. The Federal Trade Commission has already provided excellent guidelines for consumers to utilize to deter identity theft. Company Name has adopted this as a system of recommendations.

Advising Consumers on Strategies to Deter Identity Theft

Protect your personal computer, laptop, PDA, and mobile phone with passwords
Do not use PIN numbers or passwords that are easily guessed (e.g., birthdays, your maiden name, your kids' names, your pet's name, etc.)
Shred sensitive documents before placing them in the trash
Use a locked mailbox or a Post Office Box for your snail mail
Do not leave documents with your personal data laying around, especially documents with your bank account numbers or social security number
Monitor your online accounts (e.g., bank, credit card, retirement, and othe financial accounts) for suspicious or unauthorized activity
Move your paper financial statements to online accounts. Avoid paying bills with checks, and instead pay via online banking
Review your credit reports at least once a year. You can visit annualcreditreport.com or call toll-free at (877) 322-8228

Working With Borrowers Who Have Identity Theft Problems

Our obligation to our clients, when it comes to potential discovery of red flags, is to alert and provide standard direction as to potential solutions. In the mortgage industry we have very close contact with our customers. Within the mortgage application process that contact can be daily until consummation of the transaction. With this type of relationship is very easy to rely on verbal communication of the issues. It is important, when we are dealing with identity theft problems, that we provide written communication to document our efforts in assisting the applicant.

Remediation Solutions

Provide account monitoring service
Change passwords or security codes
close account and reopen with new account number
notify law enforcement – police report/SARS

Procedure upon Red Flag Alert

Step	Responsible party	Description
Review for potential red flag	Loan originator or loan processor	Utilizing the application setup or submission checklists review information and loan file
Discovery of potential red flag	Loan originator or loan processor	Identify and copy red flag document, credit report, or other evidence
Report to management	Loan originator or loan processor	Provide documents supporting red flag report to operations manager, branch manager or company official
Review documentation for potential action	Operations manager, branch manager or company compliance official	Review red flag information and determine if flag is caused by 1.) applicant as a victim of identity theft or fraud, or 2.) applicant is a perpetrator of identity theft or fraud
If Applicant is a victim of identity theft or fraud		
Notification letter	Operations manager branch manager or company compliance official	Draft red flag notification, advise loan originator in processor by copy of letter, and deliver written notification to borrower.
Complete identity theft report form	Customer, applicant or borrower	Complete the identity theft report, have notarized, and deliver to the creditors who report the new account or fraudulent account
If the applicant is a perpetrator of identity theft or fraud		
Deliver file to quality control department	Operations manager, quality control manager branch manager or compliance official	Assemble complete copy of file highlighting identity theft red flag information and request complete audit of file
Mark a file status as pending in loan origination system.	Operations manager, branch manager, quality control manager or compliance official	Identify file status as pending.
Complete “suspicious activity report” form	Operations manager branch manager quality control manager or compliance official	SAR report is completed pending receipt of findings from quality control

Preparing The Identity Theft Affidavit-Police Report

ID Theft Affidavit

Victim Information

1. **My full legal name is** _____
   (First) (Middle) (Last) (Jr., Sr., III)
2. (If different from above) **When the events described in this affidavit took place, I was known as**
   _____
   (First) (Middle) (Last) (Jr., Sr., III)
3. **My date of birth is** _____
   (Day/month/year)
4. **My social security number is**_____
5. **My driver's license or identification card state and number are**_____
6. **My current address is** _____

   City _____ **State** _____ **Zip Code** _____
7. **I have lived at this address since** _____
   (Month/year)
8. (If different from above) **When the events described in this affidavit took place, my address was**
   _____

   City _____ **State** _____ **Zip Code** _____
9. **I lived at the address in # 8 from** _____ **until** _____
   (Month/year) (Month/year)
10. **My daytime telephone number is** (____)_____

    My evening telephone number is (____)_____

    Name _____ ***Phone number*** _____

ID Theft Affidavit Continued on Next Page….

How the Fraud Occurred

Check all that apply for items 11 - 17:

11. ☐ I did not authorize anyone to use my name or personal information to seek the money, credit, loans, goods or services described in this report.
12. ☐ I did not receive any benefit, money, goods or services as a result of the events described in this report.
13. ☐ My identification documents (for example, credit cards; birth certificate; driver's license; social security card; etc.) were ☐ stolen ☐ lost on or about _____.
    (Day/month/year)

14. ☐ To the best of my knowledge and belief, the following person(s) used my information (for example, my name, address, date of birth, existing account numbers, social security number, mother's maiden name, etc.) or identification documents to get money, credit, loans, goods or services without my knowledge or authorization:

Provide any information you have regarding any persons you suspect may have used you account information. If you do not have specific contact information state: **UNKNOWN**	
Name:	**Name**:
Address:	**Address**:
Phone Numbers:	**Phone Numbers:**
Additional Info:	**Additional Info:**

15. ☐ I do NOT know who used my information or identification documents to get money, credit, loans, goods or services without my knowledge or authorization.

16. ☐ Additional comments: (For example, description of the fraud, which documents or information were used or how the identity thief gained access to your information.)

(Attach additional pages as necessary.)

Name _____ **Phone number** _____

Victim's Law Enforcement Actions

17. (Check one) I ☐ am ☐ am not willing to assist in the prosecution of the person(s) who committed this fraud.

18. (Check one) I ☐ am ☐ am not authorizing the release of this information to law enforcement for the purpose of assisting them in the investigation and prosecution of the person(s) who committed this fraud.

19. (Check all that apply) I ☐ have ☐ have not reported the events described in this affidavit to the police or other law enforcement agency. The police ☐ did ☐ did not write a report.

If you have contacted the police or other law enforcement agency, please complete the following:	
Agency:	Person who took the report:
Date of Report:	
Phone No.	Email Address (if known)
Agency:	Person who took the report:
Date of Report:	
Phone No.	Email Address (if known)

Documentation Checklist

Please indicate the supporting documentation you are able to provide to the companies you plan to notify. Attach copies (NOT originals) to the affidavit before sending it to the companies.

20. ☐ A copy of a valid government-issued photo-identification card (for example, your driver's license, state-issued ID card or your passport). If you are under 16 and don't have a photo-ID, you may submit a copy of your birth certificate or a copy of your official school records showing your enrollment and place of residence.

21. ☐ Proof of residency during the time the disputed bill occurred, the loan was made or the other event took place (for example, a rental/lease agreement in your name, a copy of a utility bill or a copy of an insurance bill).

22. ☐ A copy of the report you filed with the police or sheriff's department. If you are unable to obtain a report or report number from the police, please indicate that in Item 19. Some companies only need the report number, not a copy of the report. You may want to check with each company.

Name _____ ***Phone number*** _____

Signature

I declare under penalty of perjury that the information I have provided in this affidavit is true and correct to the best of my knowledge.

_____ _____
(Signature) (Date signed)

Knowingly submitting false information on this form could subject you to criminal prosecution for perjury.

_____
(Notary)

[Check with each company. Creditors sometimes require notarization. If they do not, please have one witness (non-relative) sign below that you completed and signed this affidavit.]

Witness:

_____
(Signature) (Printed name)

_____
(Date) (Telephone number)

Name _____ ***Phone number*** _____

Fraudulent Account Statement

Completing this Statement
• Make as many copies of this page as you need. **Complete a separate page for each company you're notifying and only send it to that company.** Include a copy of your signed affidavit. • List only the account(s) you're disputing with the company receiving this form. **See the example below.** • If a collection agency sent you a statement, letter or notice about the fraudulent account, attach a copy of that document (**NOT** the original).

I declare (check all that apply):

☐ As a result of the event(s) described in the ID Theft Affidavit, the following account(s) was/were opened at your company in my name without my knowledge, permission or authorization using my personal information or identifying documents:

Creditor Name/Address	Account No.	Type of Unathorized use	Date issued or opened	Amount or value
Example Example National Bank 22 Main Street Columbus, Ohio 22722	01234567-89	Auto loan	01/05/2000	$25,500.00

☐ During the time of the accounts described above, I had the following account open with your company:

Billing name _____

Billing address _____

Account number _____

Completing A Suspicious Activity Report (SAR)

Suspicious Activity Report

July 2003
Previous editions will not be accepted after December 31, 2003

ALWAYS COMPLETE ENTIRE REPORT (see instructions)

1

FRB:	FR 2230	OMB No. 7100-0212
FDIC:	6710/06	OMB No. 3064-0077
OCC:	8010-9,8010-1	OMB No. 1557-0180
OTS:	1601	OMB No. 1550-0003
NCUA:	2362	OMB No. 3133-0094
TREASURY:	TD F 90-22.47	OMB No. 1506-0001

1 Check box below only if correcting a prior report.
☐ Corrects Prior Report (see instruction #3 under "How to Make a Report")

Part I Reporting Financial Institution Information

2 Name of Financial Institution | 3 EIN

4 Address of Financial Institution | 5 Primary Federal Regulator
a ☐ Federal Reserve d ☐ OCC
b ☐ FDIC e ☐ OTS
c ☐ NCUA

6 City | 7 State | 8 Zip Code

9 Address of Branch Office(s) where activity occurred ☐ Multiple Branches (include information in narrative, Part V)

10 City | 11 State | 12 Zip Code | 13 If institution closed, date closed ___/___/___ (MM DD YYYY)

14 Account number(s) affected, if any
a _____ ☐ Yes ☐ No (Closed?)
b _____ ☐ Yes ☐ No (Closed?)
c _____ ☐ Yes ☐ No (Closed?)
d _____ ☐ Yes ☐ No (Closed?)

Part II Suspect Information ☐ Suspect Information Unavailable

15 Last Name or Name of Entity | 16 First Name | 17 Middle

18 Address | 19 SSN, EIN or TIN

20 City | 21 State | 22 Zip Code | 23 Country

24 Phone Number - Residence (include area code) ( )
25 Phone Number - Work (include area code) ( )

26 Occupation/Type of Business | 27 Date of Birth ___/___/___ (MM DD YYYY) | 28 Admission/Confession? a ☐ Yes b ☐ No

29 Forms of Identification for Suspect:
a ☐ Driver's License/State ID b ☐ Passport c ☐ Alien Registration d ☐ Other _____
Number _____ Issuing Authority _____

30 Relationship to Financial Institution:
a ☐ Accountant d ☐ Attorney g ☐ Customer j ☐ Officer
b ☐ Agent e ☐ Borrower h ☐ Director k ☐ Shareholder
c ☐ Appraiser f ☐ Broker i ☐ Employee l ☐ Other _____

31 Is the relationship an insider relationship? a ☐ Yes b ☐ No
If Yes specify: c ☐ Still employed at financial institution e ☐ Terminated
d ☐ Suspended f ☐ Resigned

32 Date of Suspension, Termination, Resignation ___/___/___ (MM DD YYYY)

Part III Suspicious Activity Information 2

33 Date or date range of suspicious activity
From ____ / ____ / _____ (MM / DD / YYYY) To ____ / ____ / _____ (MM / DD / YYYY)

34 Total dollar amount involved in known or suspicious activity
$ .00

35 Summary characterization of suspicious activity:

- a ☐ Bank Secrecy Act/Structuring/ Money Laundering
- b ☐ Bribery/Gratuity
- c ☐ Check Fraud
- d ☐ Check Kiting
- e ☐ Commercial Loan Fraud
- f ☐ Computer Intrusion
- g ☐ Consumer Loan Fraud
- h ☐ Counterfeit Check
- i ☐ Counterfeit Credit/Debit Card
- j ☐ Counterfeit Instrument (other)
- k ☐ Credit Card Fraud
- l ☐ Debit Card Fraud
- m ☐ Defalcation/Embezzlement
- n ☐ False Statement
- o ☐ Misuse of Position or Self Dealing
- p ☐ Mortgage Loan Fraud
- q ☐ Mysterious Disappearance
- r ☐ Wire Transfer Fraud
- t ☐ Terrorist Financing
- u ☐ Identity Theft
- s ☐ Other _____ (type of activity)

36 Amount of loss prior to recovery (if applicable)
$ .00

37 Dollar amount of recovery (if applicable)
$ .00

38 Has the suspicious activity had a material impact on, or otherwise affected, the financial soundness of the institution?
a ☐ Yes b ☐ No

39 Has the institution's bonding company been notified?
a ☐ Yes b ☐ No

40 Has any law enforcement agency already been advised by telephone, written communication, or otherwise?

- a ☐ DEA
- b ☐ FBI
- c ☐ IRS
- d ☐ Postal Inspection
- e ☐ Secret Service
- f ☐ U.S. Customs
- g ☐ Other Federal
- h ☐ State
- i ☐ Local
- j ☐ Agency Name (for g, h or i) _____

41 Name of person(s) contacted at Law Enforcement Agency

42 Phone Number (include area code)
( )

43 Name of person(s) contacted at Law Enforcement Agency

44 Phone Number (include area code)
( )

Part IV Contact for Assistance

45 Last Name

46 First Name

47 Middle

48 Title/Occupation

49 Phone Number (include area code)
( )

50 Date Prepared
____ / ____ / _____ (MM / DD / YYYY)

51 Agency (if not filed by financial institution)

Community Outreach

In order to facilitate a greater understanding of identity theft and identity fraud in the community, Company Name will support the hosting of "protect your identity day" seminars throughout our marketplace. Seminar content will be based on the Federal trade commission recommendations as contained in their pamphlet "Red Flag-Protect Your Identity Day".

Section 7 – Approval, Implementation and Revision of the Red Flag Policy

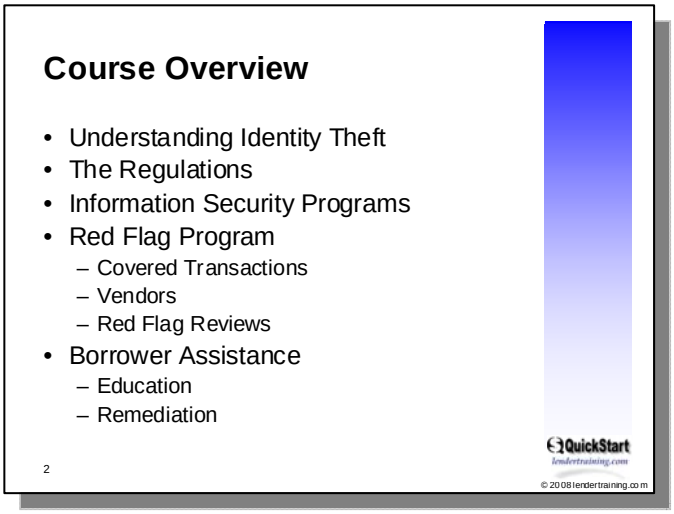
Company Name hereby accepts and adopts this red flag policy and incorporated into its daily operations. The law requires regular updating of this procedure.

Responsible Person

(Insert Name of Compliance Manager or Member Here)

Initial Training

Company Name provides a complete compliance training program for all employees, but specifically provides an update program for the training of all employees on the Red Flag Identity Theft Program.



Updating the policy

To facilitate the maintenance and updating of this red flag policy, we establish a committee comprised of the following individuals or members:

- Origination
- Processing
- Closing/Funding
- Underwriting
- Wholesale Operations
- Quality Control Compliance

The review and update of the policy includes factors that reflect changes in risk, such as:

Updating the Program "periodically" to reflect changes in risk, based on factors such as:

- Experience with identity theft
- Changes in methods of identity theft
- Changes in methods to detect prevent or mitigate
- Changes in type of accounts
- Changes in business arrangements with service providers and vendors.

Third Party Audit Firm

We may utilize an outside service in order to maintain our procedures in compliance with current conditions and laws.

(Insert Name, Address and Contact Information for Audit Firm)