Privacy Policy

Due to the nature of the Mortgage Industry and the business of C2 Financial, the employee's will come into possession of borrower's non-public personal information in the course of their day to day duties. This policy document dictates how such information will be handled and controlled in accordance with application regulations and best practices. This policy is also governed by 15 USC 6801-6809 and the Safeguards Rule of the Gramm Leach Bliley Act.

For the purposes of this policy document, the following definitions apply:

Definitions (as stated in 16 CFR 313.3):
Nonpublic Personal Information ("NPI"): any information a person gives that is nonpublic and personally identifiable to either obtain a product or service of a financial institution. This includes: name, address, income, SSN, information received from a transaction involving the financial product or service offered, and any list, description, or other grouping of consumers derived using any personally identifiable information that is not publicly available.

Publicly Available Information: any information that a financial institution has a reasonable basis to believe is lawfully made available to the general public from Federal, State or local government records, through widely distributed media or via disclosures to the general public required by Federal, State, or local law.

Examples:
The following are examples of NPI and publicly available information. These lists are not to be considered all-inclusive:

NPI:

- Fact that someone is the customer of a particular financial institution
- Consumer's name, address, social security number, account number
- Information provided on a mortgage application
- Information on a credit report

Publicly Available Information:

- Information obtained through a title search
- Borrower's name, address and telephone number obtained from a phone book
- The fact that a borrower has a mortgage on a property

Responsibility:
All C2 Financial employees and contractors who may come in contact with NPI are responsible for reviewing, learning and acting in accordance with these policies and procedures. The Information Security Plan Coordinator is responsible for ensuring compliance with these policies and procedures.

Information Security Plan Coordinator

C2 Financial has designated an Information Security Policy Coordinator. This individual must work closely with management and outside consultants, if necessary.

The Coordinator must:

- Help the company identify reasonably foreseeable internal and external risks to the security, confidentiality and integrity of borrower information.
- Evaluate the effectiveness of the current safeguards for controlling these risks.
- Design and implement a safeguards program, and regularly monitor and test the program.
- Maintain a list of employees and contractors who may have access to NPI.
- Ensure the loan originators have a full understanding of and are in compliance with such policies and procedures.
- Coordinate with divisions within the corporation to limit access to and the control of NPI.
- Coordinate with Legal Counsel to ensure these policies and procedures are up to date in accordance with appropriate regulations and laws.

In order to protect the security and integrity of the company network and its data, the Coordinator will develop and maintain a registry of all computers attached to the network. This registry will include, where relevant, IP address or subnet, physical location, operating system, intended use, the person or department primarily responsible for the machine and whether or not the machine has special access to any confidential data covered by relevant external laws or regulations.

The Coordinator will undertake the responsibility of assuring that patches for operating systems or software are reasonably up to date, and will keep records of patching activity. The Coordinator will review the procedures for patches to operating systems and software, and will keep current on potential threats to the network and its data. Risk assessments will be updated quarterly.

The Coordinator, working in cooperation with management, will develop and maintain a data handbook, listing those persons or offices responsible for covered data and will conduct ongoing audits of activity and will report any significant questionable activities to management. The Coordinator will work with Human Resources to keep this list of personnel up to date.

The Coordinator will assure the physical security of all servers or terminals that contain or have access to covered data and information. The Coordinator will also examine the physical security of paper files that contain covered data.

If applicable, the Coordinator will develop a plan to ensure that all electronic covered information is encrypted in transit and that the central databases are strongly protected from security risks.

The Coordinator will develop a plan and procedure to detect any actual or attempted attacks on covered systems and will develop incident response procedures for actual or attempted unauthorized access to covered data or information.

Training:
All employees and contractors who may come in contact with NPI will receive training prior to receiving NPI. Additionally, no less than yearly or when deemed appropriate all employees and contractors who may come in contact with NPI will review policies and procedures concerning the handling and control of NPI.

Employee Management and Training:
Recognizing that the success or failure of the Information Security Plan depends largely on the employees who implement it, the company will do the following:

- Check references prior to hiring employees/independent contractors who will have access to borrower information.
- Include a strict confidentiality provision in employment/independent contractor agreements.
- Train employees to take basic steps to maintain the security, confidentiality and integrity of borrower information, such as:
    - Lock rooms and file cabinets where paper records are kept
    - Computers: Use password-activated screensavers; use strong passwords (at least 8 characters long), require the changing of passwords periodically, and not posting passwords near employee's computers
    - Encrypting sensitive borrower information when it is transmitted electronically over networks or store online
    - Referring calls or other requests for borrower information to designated individuals who have had safeguards training
    - Recognizing any fraudulent attempt to obtain borrower information and reporting it to appropriate law enforcement agencies
- Management will instruct and regularly remind all employees of the company's policy – and the legal requirement – to keep customer information secure and confidential.
- Access to borrower information will be limited to employees who have a business reason for seeing it.
- Disciplinary measures will be imposed for any breach.

Identifying and Assessing Risks:
Risks to customer information with regards to C2 Financial include:

- Mishandling by staff
- Theft by visitors to office
- Loan Originators mishandling NPI
- Lost or Stolen computers, PDA's, cell phones, etc. that are used in the normal course of business and may contain NPI
- System Failures

Control of NPI and Safeguards:
The control of NPI relies on the diligence of those in possession of it as well as systems and policies which limit access and safeguard the information in possession of C2 Financial.

Examples of Consumer Information which may contain NPI that is within the Possession of C2 Financial:

- Hard Copies of Loan Files
- Electronic Copies of Loan Files
- Print outs of sections of Loan Files
- Appraisals
- Credit Reports
- Etc.

Hard Copy's of Loan Files/Other Documents:
When C2 Financial, corporate office receives a hard copy loan file, it should be immediately logged in and given to the person responsible for review of such file. This person should then ensure that the file is placed in a secure location when not being reviewed and ensure that it is not left in plain sight or out unattended.

All Hard copies of documents that are either received or printed shall be stored under lock and key until such time as they are no longer needed and the file is no longer being worked on.

At this time all hard copies of documents are to be scanned and saved to a secure hard drive. Once the file has been electronically stored for record retention the hard copy of the file is to be shredded.

All efforts should be made to minimize the time files/documents are out in the open and all staff shall be aware and cognizant of their surroundings and the fact that they have NPI in their possession.

Electronic Copy's of Loan Files/Other Documents:
Upon receipt and review of hard copies of loan files, they will be scanned and electronically stored. These files shall be stored on a secure hard drive with password protected access.

Individuals shall be granted access to specific restricted drive through a password protected system. This access shall be granted by the Information Security Plan Coordinator.

If individuals are accessing NPI and working in locations outside of the office, they are required to ensure that such NPI is protected and the security of such is maintained as it would be in the office. This includes not accessing NPI in public locations, ensuring laptops, PDA's, cell phones, etc are secure and password protected and they are stored in a secure place when not in use.

No less than annually, the Information Security Plan Coordinator will perform an audit of workspaces and file accesses to ensure NPI is being controlled in accordance with these procedures.

In addition upon hiring of an individual who will be working with NPI, they will receive a copy of this policy, instructions on how to treat NPI and they are required to sign a confidentiality and security standard agreement.

Managing System Failures:
The company will maintain up-to-date and appropriate programs and controls by:

- Following a written contingency plan to address any breaches of physical, administrative or technical safeguards.
- The Coordinator will check with software vendors regularly to obtain and install patches that resolve software vulnerabilities.
- The Coordinator will ensure that all anti-virus software is updated regularly
- The Coordinator will maintain up-to-date firewalls.
- The Coordinator will provide central management of security tools for employees and will pass along updates about any security risks or breaches to employees.
- All information will be backed up regularly.

Service Providers:
The company will take steps to select and retain service providers that are capable of maintaining appropriate safeguards of borrower information and will require these service providers by contract to implement and maintain sufficient safeguards to comply with the GLB Act.

Federal law mandates that this Privacy Policy be subject to periodic review and adjustment. The most frequent of these reviews will occur within Senior Management. The Plan will be reviewed no less than annually in order to assure ongoing compliance with existing and future laws and regulations.

History:

Date	Drafted By	Version/Notes
Jan 1, 2013	Noelle Pepper	V. 1