

Know
your member

Protect
your credit union



Identity
Theft
Fraud Prevention
Practices

This program is part of a comprehensive loss prevention effort from:
The Credit Union Bonding Program and the **National Risk Management Committee**



Identity Theft

Fraud Prevention Practices

In 2005, the National Risk Management Committee (NRMC) met to discuss the issue of identity theft and its impact on the credit union system and its membership. As discussions continued, it became apparent that credit unions must know their members and their financial habits intimately to fully protect themselves from the consequences of identity theft.

A result of these discussions is this ***Know Your Member, Protect Your Credit Union*** guide. This guide is meant to educate you on the risks surrounding the issue of identity theft.

How well do you and your employees know your credit union members? Knowledge is power and your understanding of your membership gives you the strength to protect your credit union from the threats of Identity Fraud. Using your knowledge and Fraud Prevention Practices, you can identify and stop fraudulent transactions before they create losses for you and your members.

What is identity theft? It's a scheme by which financial or other private information is stolen or invented, in order to make purchases or gain access to financial accounts.

Trends indicate that Identity theft is a growing problem:

- In 2005, over 11,000 Canadians reported that they were victims of identity theft, with a dollar loss suffered in excess of \$8,000,000 (source: www.phonebusters.com)
- During 2005, The Credit Union Bonding Program (TCUBP) experienced over \$1,700,000 in forgery claims. This is in addition to any credit union deductibles or Master Policy Pool deductibles (source: TCUBP Loss Extract Dec. 2005)
- By hijacking the trusted brands of well-known financial institutions, retailers and credit card companies, phishers are able to convince up to 5% of recipients to respond to them (source: Member Scam Protection brochure - Credit Union Central of Canada)
- The Canadian Institute of Mortgage Brokers and Lenders makes a conservative estimate that mortgage fraud leads to \$300-\$500 million in losses each year (source: www.cimbl.ca)

Identity Fraud can lead to a broad array of losses for your credit union, including:

- Cheque forgery
- Mortgage or loan fraud
- Plastic card or online banking losses
- A diminished reputation due to members' losses

We've created this guide to provide you with some general information on what your credit union can do to reduce the risk of loss due to identity theft. You'll find information on Fraud Prevention Practices in the areas of: Cheque Forgery, New Account Fraud, Mortgage Fraud and Online Banking Fraud.

These Fraud Prevention Practices are not all-encompassing, but they will provide you with a reference point to evaluate your credit union's current practices and identify areas where changes may be necessary. We are confident that they will assist you in creating a well-rounded risk management approach at your credit union.

These Fraud Prevention Practices are provided as a source of general information to assist your credit union in developing its own practices and procedures. However, these suggested practices do not address all possible types of fraud, nor will insurance coverage protect your credit union against all types of fraud loss.

While the information contained herein was obtained from sources believed to be reliable, we cannot represent that it is accurate or complete and it should not be considered legal or compliance advice. We are not legal advisors and we recommend credit unions seek independent advice from a professional advisor on all legal and compliance related matters.



Cheque Forgery

Fraud Prevention Practices

Cheque forgery is a significant problem for financial institutions. The good news is that with diligence, the majority of losses from cheque forgery can be avoided.

With any cheque forgery scheme, the goal of the perpetrator is to obtain cash from the financial institution prior to the fraudulent cheque being discovered. Schemes are limited only by the imagination of the perpetrator.

Types of schemes can involve:

- Counterfeit cheques
- Altered cheques
- Forged drawer's signature
- Forged endorsement
- Impersonation
- NSF cheques
- Cheque kiting

Cheque forgery can lead to significant losses for a credit union. Having a disciplined approach can greatly mitigate this risk. This document provides a summary of Fraud Prevention Practices that have been shown to reduce your credit union's exposure to cheque forgery. It is divided into two areas: Fraud Prevention Practices for Management, and Fraud Prevention Practices for Front-line Staff.

Management

Fraud Prevention Practices

Management policies create the foundation for cheque forgery risk management. The building blocks of this policy should include:

1. Documented procedures
2. Policies for cheque holds

I. Documented procedures for cheque cashing

Credit union management should ensure that cheque handling procedures are adequately documented. You should consider all of the touch points that a cheque goes through.

The documented procedures should incorporate details on:

- Front-line staff handling procedures
- Procedures for cheques deposited via ABM, including adherence to your network's operating rules. Failure to adhere to these rules can cause losses to the credit union
- Authority limits for individual staff and the referral protocol. This will include the maximum dollar value per cheque that individuals have the authority to accept, and to whom larger cheques should be referred
- Procedures for handling third-party cheques
- The handling of returned items and how to return items to others. Special attention should be made to match this to the Canadian Payments Association (CPA) rules in order to ensure that items that can be returned are returned in the proper timeframe
- The policies for holds that are to be placed on cheques
- The proper handling of incoming clearings and non-posted items
- The use of the banking system to flag unusual transactions on members' accounts. The exception report should be reviewed on a daily basis
- The physical security of the blank cheque stock
- The monitoring and auditing of the procedures in place

The documented procedures should be reviewed and approved by senior management. Procedures should be reviewed annually or whenever a significant cheque forgery incident occurs.

2. Policies for cheque holds

The longer a hold is placed on a cheque prior to releasing the funds, the less likely that a cheque forgery will be successful.

The length of time of that a cheque is held must be weighed in the context of business requirements. From a business standpoint, members cashing legitimate cheques wish to have access to the funds immediately. Perpetrators will attempt to take advantage of this business requirement by withdrawing funds prior to a fraudulent cheque being discovered.

Defining a “reasonable hold” is subjective. However, based on industry experience, the following timeframes will provide reasonable protection against cheques that are not honoured by the other financial institution (e.g. NSF, counterfeit, cannot trace):

- Within your province - three to five business days
- Outside your province - 10 to 14 business days
- Outside Canada - consider sending on collection or holding at least 30 days (even longer if outside the USA or Europe)

If, for business reasons, a hold can't be placed on cheques for this timeframe, the credit union should treat the situation as if they're offering the member unsecured credit. They must be comfortable that the member is willing and able to repay the amount if the funds aren't received from the other financial institution.

Your credit union procedures may implement a stepped approach based upon the risk that the cheque is a forgery, for example:

Personal Members

- For new members, a 10-business-day hold is applied on all cheques
- For established members, no hold is applied on cheques less than \$2500 that are drawn from a Canadian financial institution
- For all other cheques, a five-business-day hold applies
- For foreign cheques, a 30-business-day hold applies

Commercial Members

- For new members, a 10-business-day hold is applied on all cheques
- For established members, no hold is applied on cheques less than \$2500. For larger cheques, a line of credit or a loan with sufficient collateral must be established
- For all other cheques, a five-business-day hold applies
- For foreign cheques, a 30-business-day hold applies

The credit union's hold policy should be documented and strictly enforced.

Front-line Staff

Fraud Prevention Practices

The best place to reduce losses from forged cheques is at the front-line level. Since staff members manage cheques on a transactional basis, they're in the best position to identify any suspicious items. Your staff should be trained in order to meet the needs of your customers, while at the same time providing control against forged cheques.

Staff should be trained in the following:

1. Procedures for handling cheques
2. How to scrutinize cheques
3. The performance of further review checks
4. The matching of a transaction to a member's profile

I. (a) Procedures for handling cheques deposited in person

All staff should know the basic procedures for handling cheques. Procedures should be documented and followed consistently.

Procedures should include (but not be limited to) the following:

- All cheques should be reviewed for date, sum payable matching in the figure and words, and the payee name matching the endorsement
- The endorsement signature should be done in the presence of the credit union staff member. If the cheque is already endorsed, the member should be asked to re-sign the cheque in the presence of the staff member
- Proper referral protocol and authority limits should be in place
- A threshold amount for cheques should be in place over which additional steps should be taken to verify the cheque
- Cheques should be reviewed against an up-to-date fraud alert list (if available)
- Third-party cheques should be accepted with extreme caution, subject to the credit union's procedures
- Details on how staff handle suspicious cheques. Money shouldn't be released when a cheque is suspicious. Police should be contacted if appropriate. Note that your member may be an innocent victim of a scam

- Credit Union cheque hold procedures need to be strictly followed
- Communication with the member on the process and why it is important. For example, tell your member that a cheque hold will be placed

Staff should be watchful in instances where a member is pushing to bend the rules. Perpetrators will attempt to influence the process to get the cheque cashed.

1(b). Cheques deposited via ABM

Perpetrators frequently utilize ABMs to make deposits of fraudulent cheques. The same procedures as for handling the deposit of cheques in person should be strictly followed.

2. How to scrutinize cheques

Available technology makes it easy for perpetrators to alter or produce counterfeit cheques. It's nearly impossible to visually detect a high-quality forgery - and many counterfeit or altered cheques are of high quality. However, industry experience has shown that some forged cheques that are passed aren't of high quality. For these, there are usually somewhat obvious signs that the cheque isn't real.

Cheques should be examined for the following telltale signs:

- Misspelled words - including payee, financial institution, city names, etc.
- Lack of perforation on at least one edge of the cheque
- Corporate cheques for larger amounts that don't have dual signatures
- Different handwriting styles on the cheque
- Cloudy or bleached areas or erasure marks
- Writing in heavy felt-tipped pen
- Irregular fonts on a printed cheque
- Stars (***) before or after the dollar amounts
- Inconsistent or unusual fonts
- Inconsistent gaps or cramping in the printing - especially in the amounts section
- Misaligned letters or words
- Ink that looks shiny or feels raised. Tilt the cheque so it reflects light and examine the ink. Genuine printed ink is usually dull - whereas colour copier ink usually reflects light

- Does the MICR encoding make sense?
 - i. Cheque number matches the pre-printed cheque number
 - ii. Financial Institution code and transit number match real institutions and branches
- Review any security features of the cheque (for example, micro-printing)

3. The performance of further checks

If there are suspicions about the cheque or if it exceeds the dollar threshold established at the credit union, additional checks should be made prior to releasing any funds.

Steps of further review include:

- Confirm that the cheque issuer is an actual person/company independent of the information on the cheque (e.g. websites, Canada 411, Yellow Pages). The name, address and phone number should match
- Consider contacting the cheque issuer to confirm that the cheque amount and the payee match the cheque issuer's records. Obtain the phone number from an independent resource and not the number printed on the cheque. Document the name, position, and phone number of the individual contacted
- Confirm the financial institution from which the cheque is issued exists (e.g. websites, Canada 411, Yellow Pages). Confirm the transit number exists by checking a Canadian Payments Association Directory
- Consider contacting the issuing financial institution to confirm that the account exists and that there are funds available. Obtain the phone number from an independent resource and not the number printed on the cheque. Document the name, position and phone number of the individual contacted
- Obtain identification from the individual cashing the cheque. Picture identification is preferred. Compare the signature on the identification to the cheque endorsement. Compare the signature to the signature card on record. The signature should be done in the presence of the credit union staff member

It's a good practice to have these cheques reviewed a second time by an additional credit union employee.

4. Matching the transaction to your member's profile

Staff should ask themselves, "Does this cheque match the established pattern of transactions of our member?"

Obviously the better you know your member, the easier it will be to identify unusual cheques. Some red flags to consider are:

- A cheque with an amount payable that is unusually large, e.g., a member depositing a cheque of \$100,000 into an account that has never seen anything close to that amount
- An increased frequency of cheques
- Cheques from out of country or in different currencies
- Cheque issuers which don't make sense, e.g., an Employment Benefits cheque where you know the individual is fully employed; a tax return cheque being cashed in August; company cheques where it's unlikely that your member would do business with such an organization
- Sudden cheque deposits on inactive accounts. In this case, the perpetrator may be attempting to take advantage in changes in monitoring done on new accounts

It's important that scrutiny of cheques and handling procedures are maintained at all times, even when the person cashing it is a good and longstanding member. Perpetrators are very good at establishing a trusting relationship which they can exploit later. As well, your member may be a victim of cheque fraud. These procedures will protect both the member and the credit union from fraud.

These Fraud Prevention Practices are provided as a source of general information to assist your credit union in developing its own practices and procedures. However, these suggested practices do not address all possible types of fraud, nor will insurance coverage protect your credit union against all types of fraud loss.

While the information contained herein was obtained from sources believed to be reliable, we cannot represent that it is accurate or complete and it should not be considered legal or compliance advice. We are not legal advisors and we recommend credit unions seek independent advice from a professional advisor on all legal and compliance related matters.



New Account Fraud

Fraud Prevention Practices

Getting new members to join your credit union is an important part of growing your success. However, if your new member is only opening the account to later defraud the credit union, you don't want their business!

A typical new account fraud scheme may unfold like this:

Someone walks into your credit union and asks to open an account. The member service representative, following credit union policy, requests a driver's license and another form of identification. The representative verifies the name on the driver's license matches the Social Insurance Number card, and the photo matches the person sitting in front of them.

The applicant passes the screening and the member service representative shakes hands and congratulates the individual on becoming a member.

Three months later, the member deposits an altered cheque for \$15,000. The funds are withdrawn before the cheque is returned to your credit union. At that time, it is determined that the applicant was using someone else's identity, and all their identification was forged.

The credit union is left holding the bag for the loss.

Most new applicants are trustworthy and will become good longstanding members for your credit union. However, there will always be individuals who will attempt to join your credit union with the intent to defraud you. With a little diligence, schemes such as the above can be identified before potential losses occur.

Fraud Prevention Practices are also important to comply with Money Laundering and Terrorist Financing legislation. This document provides a summary of Fraud Prevention Practices that have been shown to reduce your credit union's exposure to new account fraud.

Fraud Prevention Practices

Management should ensure that account opening procedures are documented and address the issues identified in the Fraud Prevention Practices.

Generally, front-line staff is in the best position to reduce losses from account opening fraud. They should know and understand credit union procedures and have, at their disposal, required tools, e.g. new account opening checklists, access to order credit reports (to assist with the process). They should also receive regular training about cheque fraud and other current fraud schemes.

Risk management against account opening fraud takes into account the following timeframes:

1. The day the account is opened - exercise extreme caution
2. The next three to six months - monitor the account and take additional safeguards
3. If anything appears suspicious - take immediate action on the account

I. Exercise caution in account opening

During the initial meeting when the account is set up, besides informing your new applicant of all the products and services your credit union offers, your member service representative is responsible to ensure that the applicant is truly who they say they are.

The process of ensuring that the applicant is truly who they say they are can be broken down into three areas:

- Obtaining proper identification
- Using independent sources to verify the identification
- Validating all of the information

Obtaining proper identification

Valid identification should be obtained for all new account openings and should include one piece of primary identification, and at least one piece of secondary identification.

Primary Identification	Secondary Identification
<p>Primary identification should:</p> <ol style="list-style-type: none"> Contain a picture; Have a signature; Have an expiry date; and Be issued by a recognized organization (<i>usually a government agency</i>) that does some investigation on identity. <p>Acceptable forms of primary identification:</p> <ul style="list-style-type: none"> Drivers license Passport Other federal/provincial issued cards that contain a photograph and signature * <p>(*in some provinces it is prohibited to use a health insurance card.)</p>	<p>Secondary identification is used to support the applicant's primary identification.</p> <p>Acceptable forms of secondary identification</p> <ul style="list-style-type: none"> Birth certificate SIN card Credit cards (<i>signed</i>) Debit cards/bank cards (<i>signed</i>) Letter of introduction (<i>only if it can be verified</i>) Certificate of Canadian citizenship, Certification of Naturalization, or Permanent Resident Card Old Age Security Card Certificate of Indian Status

The following identifications aren't considered suitable for opening an account as they are easy to obtain, easy to counterfeit, and offer no validation of identity:

- Employee cards (unless part of a closed bond credit union affiliated with that company)
- Student cards (including college/university)
- Club or association cards
- Grocery cheque cashing cards
- Marriage license
- Library cards

For business accounts, ensure that all required documentation is received, including business registration, certificate of incorporation, and resolution appointing signing officers.

Use independent sources to verify the identification

Identification can be obtained under fraudulent pretenses or be counterfeit. The authenticity of the identification should be verified using independent sources. The more independent verifications performed, the more likely the identification is valid.

Some reliable sources to reference for identification checks are:

- Credit reports
- Employers
- On-line directories (e.g. www.411.ca) or phone books to validate address and telephone numbers
- Fraud and investigation bulletins
- Recent bills to validate residence address (e.g. utility bill)

Information provided from these sources should be compared and match the information from the identification. It is important that this information is obtained independently from what the applicant has provided.

To counteract identity theft, it is a good idea to send a “Welcome Letter” to the applicant’s address. In the case of identity theft, the recipient will likely contact your credit union once they receive this if they, in fact, have not opened the account.

Validate all the information

Once you have the identification and have verified its authenticity, the final consideration for the member service representative is to validate the information obtained. The member service representative should feel comfortable with the new member and the application.

Some questions staff members can ask themselves:

- Do the names, addresses and birthdates match on all the pieces of information?
- Does the picture on the identification match up with the applicant?
- Is all identification recently issued? (This is sometimes an indication of an identity takeover)
- Given the credit union location, does it make sense for the member to open an account with you, i.e., are there other financial institutions that are closer?
- Does the applicant seem overly eager to open the account and unconcerned about service fees?
- Is the applicant known to other members?

The member service representative should trust their intuition. If concerns still remain, more investigation should be conducted or the new member's application should be declined.

Similar diligence should be taken for any changes in member information. The information should be verified and validated in the same way.

2. Monitor the account and take additional safeguards

Newly established accounts should be monitored more closely and additional safeguards considered than with existing accounts. On newly established accounts, potential fraudsters will take the opportunity early on to explore and identify weaknesses in your credit union.

Specific monitoring may identify suspicious activity and allow the credit union to respond before a fraud occurs. Additional safeguards will limit any losses that do occur.

Specific occurrences that should be monitored on new accounts:

- Large or an unusual number of deposits
- Items returned back from clearing
- Account becoming overdrawn
- Non-branch transactions greater than \$2500
- Change of address requests (these should be independently verified)
- Returned mail
- Frequent ATM withdrawals and POS transactions
- Cheques issued by the member from another financial institution - which may be a sign of cheque kiting

Additional safeguards that should be implemented during the initial stage:

- Longer than usual holds on cheques (especially with large cheques)
- Holds on ATM deposits (at least until the deposit has been verified)
- Lower limit on ATM withdrawals and POS transactions

3. Take immediate action

When fraudsters launch their scheme, they usually attempt to withdraw as much money as they can over a short period of time. Quick reaction by the credit union can prevent or limit any loss.

In the event that any suspicions are raised:

- Refer the account immediately to a supervisor. The supervisor should immediately investigate (or assign to someone else to investigate) the suspicions
- The account should be temporarily frozen to facilitate the investigation
- The investigation should include a review of the account opening documents, a review of the transaction history, and a review of the suspicious items
- Specific attention should be placed on reviewing any recent cheques deposited into the account. These items may have initially cleared, but could still be returned if they are materially altered. See Cheque Forgery section for further information
- All suspicions should be eliminated prior to unfreezing the funds

These Fraud Prevention Practices are provided as a source of general information to assist your credit union in developing its own practices and procedures. However, these suggested practices do not address all possible types of fraud, nor will insurance coverage protect your credit union against all types of fraud loss.

While the information contained herein was obtained from sources believed to be reliable, we cannot represent that it is accurate or complete and it should not be considered legal or compliance advice. We are not legal advisors and we recommend credit unions seek independent advice from a professional advisor on all legal and compliance related matters.



Mortgage Fraud

Fraud Prevention Practices

Mortgage fraud is a significant and growing problem for lenders in Canada. Although there is no central reporting of fraud losses, a conservative estimate is that mortgage fraud leads to \$300 - \$500 million in losses each year¹. There is no easy solution to reduce or eliminate this problem.

Mortgage transactions involve several parties, each of whom plays a role in ensuring that a particular mortgage is not a fraud. Unfortunately, your credit union will usually end up suffering the majority of the financial loss if one of the parties fails in their role. In addition, fraud schemes are usually only detected when a loan goes into default. At such time, there isn't much that can be done to mitigate the loss.

Prevention of mortgage fraud requires the combined efforts of all the parties involved in the real estate and mortgage transactions. Fraudsters will target the parties where the process and the controls are the most lax. To make matters worse, fraudsters will often collude with one of the parties, making the scheme even harder to detect.

Most new mortgages that your credit union obtains are legitimate. However, since mortgage fraud can result in a significant loss to your credit union, you must diligently manage every account in order to reduce the risk.

There is no easy solution to eliminating the problem. To reduce the risk your credit union should ensure:

- that all parties are acting honestly and diligently
- that your member is acting honestly

This document provides a summary of Fraud Prevention Practices which have been identified to help you reduce the risk of mortgage fraud. These Fraud Prevention Practices are designed specifically for financial institutions. The other parties involved in the transaction that play a role in reducing risk, should implement their own Fraud Prevention Practices. (The real estate agents association, the mortgage brokers association, and the law societies have all implemented guidelines for their members.)

Fraud Prevention Practices to help avoid mortgage fraud can be divided into procedural and transaction issues. Credit union management should ensure that their mortgage procedures reflect these Fraud Prevention Practices. Individuals responsible for the day-to-day handling of mortgages should be aware of the transactional Fraud Prevention Practices.

All mortgage staff should be encouraged to become members of CIMBL and to pursue an AMP designation. For information visit <http://www.cimbl.ca/amp-designation.htm>. Note: As of May 1, 2007, CIMBL will officially be known as CAAMP (Canadian Association of Accredited Mortgage Professionals).

1 Canadian Mortgage Industry Fraud White Paper. CIMBL Mortgage Fraud Task Force, October, 2001.

Procedural Issues

Fraud Prevention Practices

Points to consider within the credit union procedures are:

1. Your knowledge and trust of other parties within the transaction
2. Your ability to ensure that other parties are being diligent in their duties on each transaction
3. The establishment of written procedures and checklists

1. Knowledge and trust of other parties

A mortgage transaction involves several parties working together. Each has an important role to play in identifying and stopping fraud. It is important that the credit union know the parties involved in the transactions and is comfortable that each can fulfill their role in the risk management process. Initiating a background research into the parties is recommended.

The chart below identifies the steps that can be taken to substantiate the various parties and for you to gain a higher comfort level with each.

Party to Transaction

Purchaser	<ul style="list-style-type: none">• Usually your member• Follow standard account opening procedures
-----------	--

Vendor	<ul style="list-style-type: none">• Usually unknown to your credit union• Informally check against known fraudsters or schemes• Watch for transactions involving unusual power of attorney <i>(for example, not an executor of an estate)</i>
--------	---

Real Estate Agents	<ul style="list-style-type: none">• The real estate agent of record is not something you can control• Informally check against known fraudsters or schemes
--------------------	---

Credit Agency	<ul style="list-style-type: none">• Credit reports should be ordered by the credit union directly. Do not rely on copies provided by others as they may have been altered
---------------	---

Party to Transaction (continued)

Mortgage Broker • Your credit union selects the mortgage brokers you wish to deal with. Due diligence should be undertaken in this selection process. Responsibilities should be documented within the contract between the credit union and the mortgage broker. Regular audits should be done to ensure that the mortgage broker is managing files as agreed

Lawyer • The choice of lawyer is out of your control

Appraiser • Your credit union usually selects the appraiser
• A list of approved appraisers should be created. On an annual basis, the list should be reviewed and updated

Title Insurer • Your credit union usually has no control over the choice of title insurer, but you may be involved in the referral process
• Title insurers may be able to identify schemes or suspicious mortgage applicants

2. Ensuring the diligence of other parties in their duties

Each of the parties involved is responsible for guarding against mortgage fraud by performing their own distinct risk management duties. A level of trust should be allotted to these parties that they are diligently fulfilling their duties. However, your credit union can take steps to ensure their performance.

On a formal basis, it is important that your credit union verify that all the proper paperwork is completed.

Informally, on a case-by-case basis, your credit union can contact the other parties, and directly ask them to confirm that they have fulfilled their duties. This is especially effective if your work has raised some potential red flags. By contacting the other parties, it will cause them to take a second look at the transaction and possibly uncover additional red flags. This may be enough to stop a fraudulent transaction.

3. The establishment of written procedures and checklists

A mortgage transaction is complex. Credit union management should ensure that mortgage handling procedures are adequately documented. The documented procedures should incorporate details on:

- Authority limits and the referral protocol
- Lists of approved suppliers (i.e. appraisers, mortgage brokers)
- List of required documentation
- List of red flags that a transaction may be fraudulent

All loans staff should be thoroughly trained and knowledgeable about these procedures. Regular audits need to be performed to ensure the procedures are being consistently followed.

Transactional Issues

Fraud Prevention Practices

If a mortgage fraud occurs, it will result in a significant loss to the credit union. As a result, it is imperative that each mortgage application be properly investigated to reduce the chance of fraud. Front-line loans staff are in the best position to identify and stop mortgage fraud.

The following are key reminders for front-line loans staff:

1. Funds should not be released until all procedures are complete
2. They need to ensure all documentation is in order
3. They need to watch out for red flags indicating a fraudulent situation

1. Do not release funds until all procedures are complete

There may be significant time pressures to release the funds in a mortgage transaction. For example, real estate transactions may be delayed or fall through if funds are not released on time. It's understandable that your credit union doesn't want to be the cause of such a delay. However, the funds should not be released until all information is received and procedures finalized. Once money is released, it's difficult to recover if the transaction proves to be fraudulent.

2. Ensure that documentation is in order

The loans officer should ensure that all documentation is in order. Some important documents that should be reviewed include:

- Fully completed application
- Identification of borrower (If more than one borrower, identification for all borrowers should be reviewed)
- Credit reports (Ensure that information is consistent with the information on the application. Watch for identity theft warnings.)
- Proof of employment
- Copy of the Agreement for Purchase and Sale
- Copy of the MLS listing
- Copy of the appraisal
- Correspondence with the solicitor

3. Watch out for Red Flags

All the information submitted as part of the application should be scrutinized for accuracy and consistency. A red flag in itself doesn't necessarily mean the application is a fraud.

The chart below identifies some red flags that may indicate the need for more intensive review.

Source of Information	Potential Red Flags (that require further review)
Mortgage Loan Application	<ul style="list-style-type: none">• Unusual source of the cash for down payment• Borrower buying an investment property, but does not own current residence• New home is not large enough/too large/not suitable for the proposed occupants• Unrealistic commute distance from property to employment• Borrower's education is inconsistent with their employment• Number of years/level of employment is inconsistent with the borrower's age• Borrower income is inconsistent with their employment• Phone numbers provided (home, work) identified as a cellular number

-
- Credit Report
- Personal data is not consistent with the application (*including name, age, address, employment history*)
 - SIN number is not the same
 - Variance in credit information
 - Credit history inconsistent with the profile of the borrower (*no credit history; several newly-opened trade lines; several recent inquiries*)
 - Fraud Alert of Identity Theft Warning

-
- Verification of Employment
- Employment verification is not on company letterhead
 - No address or contact information
 - Company phone number is a cellular number
 - Company name does not appear in any directories (*business directories, Yellow Pages, Internet*)
 - No name/position of individual signing the letter.
 - Letter appears to have been altered
 - Person verifying the information appears to be related to the borrower
 - Spelling and typographical errors
 - Pay stubs of a large employer not computer generated

-
- Purchase and Sales Agreement
- Borrower is not shown as the purchaser
 - Names have been deleted or added.
 - Location address does not match the mortgage application

-
- Solicitors Instructions/ Documents
- Changes in final sales price
 - Unusual amendments to the original transaction
 - Power of attorney used instead of a signature of the actual seller or purchaser

-
- Appraisal
- Location address does not match the mortgage application
 - Owners name does not match the Purchase and Sales Agreement
 - Photos do not match the description of the property
 - Comparable properties pricing is inconsistent, is either missing, not recent, no source provided, or not in a similar type/area of subject property
-

General Mortgage and addresses File • Inconsistencies in terms of names, phone numbers within documents
• Parties to the transaction have more than one role, for example, the realtor is the owner of the property
• Borrower's signature is different on the various documents
• Contact information is the same for various parties to the transaction, for example, the borrower and the realtor have the same phone number

Applicant • Difficult to contact the applicant on other than a cellular phone

Note: Although this document discusses mortgage fraud, similar practices can be implemented to protect against loan fraud.

These Fraud Prevention Practices are provided as a source of general information to assist your credit union in developing its own practices and procedures. However, these suggested practices do not address all possible types of fraud, nor will insurance coverage protect your credit union against all types of fraud loss.

While the information contained herein was obtained from sources believed to be reliable, we cannot represent that it is accurate or complete and it should not be considered legal or compliance advice. We are not legal advisors and we recommend credit unions seek independent advice from a professional advisor on all legal and compliance related matters.



On-line Banking

Fraud Prevention Practices

On-line banking fraud is considered a form of identity theft fraud. The perpetrator steals the on-line identity of your member in order to embezzle money. As on-line banking becomes more prevalent, attacks will increase. It is vital that your credit union implements a comprehensive program to limit the exposure to your institution and your members.

Loss control is imperative for on-line banking operations. In addition to exposure to financial loss, your credit union may be faced with a loss of consumer confidence following a security breach. Typical on-line banking schemes target your members as they are the easiest area to attack. The most common on-line banking fraud schemes that are taking place in North America are:

- Impersonation schemes, where the fraudster tries to convince the member that they are being contacted by the credit union or other legitimate party; and
- Technology schemes, where key logger, spyware or trojan horse programs are used to gain confidential information

The Fraud Prevention Practices outlined here have been shown to reduce the fraud risk associated with on-line banking operations. These practices are general in nature. Due to the technical nature of on-line banking, it's important to utilize area experts to implement your program.

Preventing On-line Banking Fraud

Your credit union should focus on reducing the threat of on-line banking fraud by following these three key principles:

1. Ensure that your systems are properly protected
 - Your credit union systems should be protected by up-to-date fire walls, virus protection, and security patches.
 - Access to your systems should be limited to those who need it.
 - Sensitive data should always be stored in encrypted format.
 - The effectiveness of your security measures should be tested regularly.
2. Educate your members
 - Members should receive frequent information about the importance of having current virus/spyware protection for their personal computers.
 - All on-line banking users should have easy access to information on how to avoid becoming the victim of phishing or other schemes where they are asked to provide on-line banking passwords.
 - Set up an e-mail group that allows you to send a fraud warning to all on-line banking users at once.
3. Real time analysis of all transactions
 - Transactions should be monitored on a 24/7 basis and be able to identify suspicious transactions in real time, and be able to revoke access to the accounts.
 - Analysis should be able to identify transactions which are unusual based upon the profile of your individual members.

More specific details regarding On-Line Banking Fraud Prevention Practices are outlined below:

General

- Understand the risk. Evaluate all new on-line services for both the probability of a security breach and the consequences of such an occurrence. E-mail money transfer and on-line Interac® services which allow transfers outside of the credit union carry substantially higher risks than on-line services that are restricted to bill payments and transfers between the member's accounts.
- Educate your members about security issues. Ensure that security information is both comprehensive and easy to read. Be clear about the responsibilities of your members. Specific areas of education should centre on phishing and the requirements for up-to-date virus protection.
- Use a well-established banking system provider, with strong technical security expertise and resources. Remember that effective IT security can be expensive, and low-cost providers may provide weak or non-existent security protection.
- Establish security measures that restrict data to those who need it, and ensure that old data is not stored after it is no longer required. Sensitive member and account information should be stored in encrypted formats.

Security Controls

- Member account access to on-line banking should only be provided after the member requests such access.
- Appropriate procedures are needed to ensure that the person requesting changes or new access to on-line banking is actually the member, particularly if you accept customer account instructions by fax, telephone or e-mail.
- If new passwords are mailed to the address of record, a process is needed to make sure the address has not recently changed.
- The banking system should be monitored for unusual activity, and a process in place for blocking accounts when suspicious transactions occur. To be effective this process should be in place 24 hours a day, 7 days a week.
- Employees should be restricted from ever receiving, entering or knowing member passwords. This reduces the risk of employee fraud.
- Member accounts should be automatically blocked after three (3) incorrect password attempts. This will help prevent automated programs from breaking passwords through repeated attempts.
- It is essential that the banking system have maximum dollar limits allowed for member transactions, especially any withdrawals or transfers out of member accounts.
- The banking system should have limitations on the frequency of transactions (for example, three per day), or an audit log should be created and reviewed for any member exceeding three transactions per 24-hour period.
- Any confidential on-line banking screens should automatically be cleared from the browser's memory and hard disk cache (history) after the user signs off or logs out.
- Members should be instructed to sign off or log out of the system rather than just using the home or back button.
- The banking system should terminate the member's online session after a period of inactivity, such as five minutes.

New Account Controls

- On-line banking applications should be made in person at the credit union branch. If that is not feasible, then security procedures for accepting membership applications over the Internet are required.
- Verify membership eligibility for new member requests, particularly if received over the Internet. Have procedures in place to verify new information on members, such as SIN and phone numbers, birth dates and addresses.
- Establish procedures to verify income, employment and credit bureau reports on loan applications received over the Internet.

On-Line Banking System

- Use an established on-line banking system provider that has a strong security protocol in place.
- Encourage your on-line banking system provider to include loss prevention material on its sign-on page.
- Establish daily cash limits on transactions involving money transfers out of the member's accounts
- Support the use of enhanced security measures for future upgrades of your on-line banking system, such as:
 - Image recognition (such as Passmark)
 - Individual PC recognition (which only allows authorized computers to access the system)
 - Key fob or similar random password generation (two factor authentication)
 - Biometrics
 - Home PC card scanners (for use with debit cards)

Web Site Security

- Your Web site should provide secure connections with the member and require encryption on all confidential data transmissions, including membership applications, loan applications, and on-line banking member information.
- Firewalls should be used to protect your internal systems if you use a direct broadband connection (a direct broadband connection is a permanent link to the Internet, such as a cable or network connection). You may need to obtain specialized IT expertise to properly configure appropriate firewalls. A process should be in place to ensure that firewalls are kept current with all vulnerability patches and upgrades installed promptly.
- Your banking system and network should ideally be continually monitored by intrusion detection software. System administration logs need to be monitored for signs of attempted security breaches.
- Anti-virus, anti-spyware and intrusion detection software, as well as your vulnerability assessment tools, need to be updated at least monthly. Vulnerability assessments should be run on a regular basis.
- Your Web site should include a digital certificate to verify its authenticity (a digital certificate is a secure electronic credential which prevents a Web site from being copied or spoofed by someone pretending to be the legitimate site).

Web Hosts / Internet Service Providers

- You should have a formal written contract with each of your vendors and service providers. The contracts must specify confidentiality requirements of member data and should include contingency plans for backups and resumption of service in the event of a system failure.
- Check to see if your vendor performed an independent information systems audit or third party security review of their system, including penetration testing of their system.
- Verify that your vendors must conduct pre-employment background checks on their employees. This should be mandatory in order to reduce the risk of vendor employee fraud or information theft.
- As a precaution against “phishing” schemes, you need to reserve all versions of your domain name (e.g. .com, .org, .net, .ca, etc.).
- Maintain backup copies of your systems, including your Web site code. This will increase your ability to quickly restore services and reduces the chance of having to re-create or re-assemble data (which is often not covered by insurance).
- Allow only the most reputable outside organizations to be linked to your Web site, and ensure that their Web site security is strong.
- Determine if your service providers provide any insurance coverage protecting the credit union against fraud involving their employees or other parties.