Great Britain Customized Data Sheets

Burglary and Robbery (SA)
Internal Control Analysis (ICA)
Forgery & Fraudulent Deposit Analysis (FFA)
Fidelity Analysis (FA)
Office Safety Analysis (OSA)

Questions to be asked at every credit union # Code and record answers and comments below!			
Manager Details			
Contact Person Details, if different form above person			
CU Address opening hours, No. Staff/volunteers & Banking arrangements			
Branch and/or collecting points			
Location, opening hours, No. Staff/volunteers, & Banking arrangements			
Organ-a-gram, BoD, Manager & Staff, volunteers			
Have any losses occurred over the past 2 years?			
Who monitors losses and files claims?			
Has the CU designated “Risk Officer” for the credit union?			
What new member service is being considered in the next 2 years?			
Are there building or remodeling plans in the next 2 years?			

BURGLARY ANALYSIS

Cash and Cheque Storage	NA	No Rec	Rec
Are cash/cheques stored on CU premises out of opening hours?			
Are cash/cheques taken off CU premises out of opening hours?			
Are the procedures for storing cash/cheques within guidelines?			
Safe/Vault			
Is any safe/vault of the appropriate rating, i.e. TL15 or better?			
Are they alarmed, door contact, heat and sound sensors?			
Are they properly/best situated in building?			
Are safe/vaults locked out of opening hours?			
Is the key/combination protected/secure?			
Records			
Are vital records stored so as to be protected up to 2hours?			
Are important records stored so as to be protected up to 1 hour?			
Are all other records stored securely and safely?			
Alarm			
Are CU premises suitably alarmed?			
Is there a secure line to alarm company/Police?			
Are safe/vaults locked out of opening hours?			

ROBBERY ANALYSIS

Transportation & Security	NA	No Rec	Rec
Is cash transferred to bank within appropriate bond limits?			
Is an armoured vehicle used where cash limits exceed £5k?			
Are appropriate concealment methods of cash transportation used?			
Is the time of banking varied?			
Do different people bank monies?			
What records of cheques banked are kept at CU?			
Are there intruder on premises (panic alarms) during opening hours?			
Are security cameras available, internal/external?			
Are there physical barriers to deter robbery, internal/external?			
Is there a maximum amount of cash to be held at counter/teller point?			
If more than one counter/teller point is cash amount divided between points?			
Additional Robbery Information			
Are staff trained in what to do in the event of a robbery?			
Are staff trained in what to do before, during and after event?			
Is the counter/teller point high/wide enough to deter vaulting?			
Are counter/teller point staff in a secure locked area?			
Are height markers suitably positioned at counter/teller point and doors?			
Are other persons on premises able to be warned a robbery is in progress?			

INTERNAL CONTROLS ANALYSIS

Basic Internal Controls	NA	No Rec	Rec
Are cash/cheques reconciled to general ledger?			
Is audit trail of cash/cheques adequate?			
Does more than one person check cash?			
Is access to cash limited?			
Are counter/teller points locked when temporarily vacated?			
Is there an appropriate control of keys?			
Is consideration given to lock changes when employee/volunteers leave?			
Do counter/tellers deal with own/family accounts?			
Are cheques deposited CU endorsed immediately?			
Is computer/ledgers access controlled?			
Does the person paying expenses also enter general ledger posting?			
Are there written procedures on corporate/personal expenses?			
What procedures are used to monitor dormant accounts?			
What procedures are in place to verify LP/LS payments?			
Are bank reconciliation carried out regularly?			
Is the access of available funds displayed to members?			
Is there a written fraud policy for employees/volunteers?			

Other Internal Controls			
Are signatures witnessed?			
Is positive proof of ID required?			
Are signatures compared to dependable documents?			
If ID checked is this suitably recorded?			
Are third party cheques able to be accepted?			
Are deposit cheques holds used, i.e. 3 days before withdrawal possible?			
Are employees/volunteers trained to spot false deposits/ID (Awareness, body language, uneasiness and what to do if detected)?			
Is there an active Supervisory Committee providing reports to Directors?			
Is an Internal Auditor used?			

FRAUDULENT DEPOSITS & FORGERY ANALYSIS

New Accounts	NA	No Rec	Rec
Are new accounts highlighted?			
Are employees/volunteers multiple accounts highlighted?			
Is new member ID verified and recorded, i.e. 2 pieces ID Money Laundering Regs.?			
Are employees/volunteers trained in new/multiple family accounts?			
Does the CU use external ID verification?			
Are there extended holds on high-risk accounts?			
Fraudulent Deposits			
Is there a written cheque hold policy?			
Is policy of availability of funds clearly displayed to members?			
Are third party cheques scrutinised and verified?			
Are checks made on large deposit cheques?			
Are tellers able to verify account balance when presented with an on-us cheque?			
Do employees/volunteers look for falsehood fraudulent behaviour?			
Member gets angry when asked for information?			
Nervous or impatient with teller?			
Unusual/temporary address?			
No phone number?			
Does not want to have cheque verified?			
Tried to distract employee/volunteer?			
Do employees/volunteers check that cheques are valid words/figures, date valid?			
Are there counter/teller audit to check adherence to guidelines?			
Are up to date SCAM alerts given to all employees/volunteers?			
Are employees/volunteers able to identify 'kiting'?			
Forgery			
Are employees/volunteers trained to spot forged documents, ID etc.?			
Bleach marks?			
Different inks?			
Erratic writing?			

Do employees/volunteers witness signatures?			
Do employees/volunteers ask for members to provide another signature in their presence?			
Do employees/volunteers when member deposits cheques made out by another person verify account with bank?			
Insurance Coverage			
Does the CU have fraudulent deposit, forgery and other alteration coverage?			
Shared Branches			
Are CU policies and procedures provided to all collection points/branches?			
Are employees/volunteers at collection point/branches able to communicate with CU office?			
Are clear instructions in place regarding the handling of cash/cheques?			
Is verification provided of deposits banked to general ledger?			

Fidelity Analysis – Great Britain

Credit Union _____ Date _____

Employee & Family Member Accounts **Journal Voucher Transfers** **Lending Exceptions**	**Dates Reviewed:_____**
Director/Officers/Appointees & Family Member Accounts **Journal Voucher Transfers** **Lending Exceptions**	**Dates Reviewed: _____**
Fictitious / Unauthorised Loans	**Dates Reviewed:_____**
Expenses	**Dates Reviewed:_____**
Deposits In Transit Audit	**Dates Reviewed:_____**
Cancelled Checks Audit	**Dates Reviewed:_____**
(a) Share Withdrawals	
(b) LP / LS Insurance Proceeds	
G/L Suspense Accounts	**Dates Reviewed:_____**
(c) CDI / CLI Payments	
(d) Closed Accounts	
(e) Dormant Accounts	
Repossessed Collateral	**Dates Reviewed:_____**
Traveller's Cheques	**Dates Reviewed:_____**

Great Britain Customized RMA Standard Answers

Burglary (SA)
Robbery (SA)
Internal Controls (ICA)
Fidelity (FA)
Office Safety (OSA)

All reports should include the following standard opening paragraph and commentary. It sets the tone for the report and it defines a recommendation and requirement.

Risk Management Analysis
Great Britain Credit Union
Main and One Collection Point Office

Several commendable procedures and security measures were observed during the analysis. This report contains a review of physical conditions, practices, and procedures that represent increased elements of risk. The recommendations and/or requirements in this report are based upon statements made to us, as well as observed exposures and/or hazardous conditions. This report does not indicate risks, not considered or observed, are adequately controlled.

Several commendable procedures and security measures were observed during the analysis. This report contains a review of physical conditions, practices, and procedures that represent increased elements of risk. The recommendations and/or requirements in this report are based upon statements made to us, as well as observed exposures and/or hazardous conditions. This report does not indicate that risks, not considered or observed, are adequately controlled.

COMMENTARY

This report may include recommendations and/or requirements. The definition for those terms is provided below:

A **recommendation** is our best advice of how to reduce loss, or the potential for loss, in a given area.

A **requirement** is a particular area of concern in which the credit union must comply with our solution, or negotiate an acceptable compromise for solution. Otherwise, underwriting action will be taken. The action could consist of lower coverage limits, higher deductibles, or a restrictive (exclusionary) endorsement.

In the written response you have agreed to submit, it is very important for the credit union to clearly indicate whether you will, or will not, adopt the individual recommendations and/or requirements.

This report may include recommendations and/or requirements. The definition for those terms is provided below:

A **recommendation** is our best advice of how to reduce loss, or the potential for loss, in a given area.

A **requirement** is a particular area of concern in which the credit union must comply with our solution, or negotiate an acceptable compromise for solution. Otherwise, underwriting action will be taken. The action could consist of lower coverage limits, higher deductibles, or a restrictive (exclusionary) endorsement.

In the written response you have agreed to submit, it is very important for the credit union to clearly indicate whether you will, or will not, adopt the individual recommendations and/or requirements.

GREAT BRITAIN RISK MANAGEMENT ANALYSIS - STANDARD ANSWER

ALL STANDARD RECOMMENDATIONS USE THE, "THIS IS THE PROBLEM AND THIS IS WHY IT'S A PROBLEM" FORMAT FOLLOWED BY AN APPROPRIATE RECOMMENDATION. RECOMMENDATIONS ARE COLLORED SO THEY CAN BE COPIED AND EDITED INTO A NORMALLY ALL BLACK DOCUMENT. WHEN DONE,

CHANGE TEXT TO BLACK. NOTE: RECOMMENDATIONS WRITTEN BY RICH ARE IN BLUE. THEY SHOULD BE TRANSLATED INTO BRITISH AND COLORED RED. RECOMMENDATIONS WRITTEN BY STEVE ARE IN RED!

BURGLARY ANALYSIS RECOMMENDATIONS

Secure Door to rear of teller area

Entry to the rear of the teller's area is via a secure door opened by way of a keypad operation, this is good practice creates a clear defendable zone for volunteers/staff. However keypad code is unable to be changed or varied at regular intervals making knowledge of said code to become widely known.

Recommendation: When appropriate upgrade keypads to one were codes can be varied and strictly limit codes to authorised persons only.

Key Cupboard

A key cabinet was located in a cupboard in the teller area. The cabinet was open and the control key in lock; all the keys were labelled as to their respective lock. This gives access to all areas of the Credit Union and would assist thieves at time of burglary.

Recommendation: The key cabinet is securely locked at all times and control key kept in other secure place. The keys to be stored without labels, but with in a coded sequence details of which to be restricted to authorised persons only.

Rear Security Door

The rear security door hinges were exposed to the exterior making access via removal of hinge pins simple.

Recommendation: Convert exterior hinge pins to secure non removable types.

Locked Container Stored in Sponsor's Safe

Volunteers at the collection point store credit union cash in the sponsor's safe. This is an acceptable practice provided the containers used are locked and the amount of cash does not exceed an amount established by credit union policy.

Recommendation: Adopt a written policy that all containers stored in the sponsor's safe are locked and keys are retained by authorized credit union staff/volunteers. Spare keys to these containers should be stored under appropriate spare key controls at the main office. Based on the burglary resistant quality of the sponsor's safe, no more than 2000 pounds should be stored in the sponsor's safe during out of opening hours. As an aside, check with the sponsor to determine what if any coverage is provided should there be a burglary or mysterious disappearance loss.

Front Door to premises

The front door to the premises is the obvious point of entry to a burglar as internal grills protect all windows. As the premises are in an isolated location and in an area not visible to passing public this risk is heightened.

Recommendation: Consider ways of securing the front doors to prevent access out of office hours. Alternatively a surveillance system covering the door should be fitted.

Locked Container Stored in Sponsor's Safe

Volunteers at the collection point store credit union cash in the sponsor's safe. This is an acceptable practice provided the containers used are locked and the amount of cash does not exceed an amount established by credit union policy.

Recommendation:

Adopt a written policy that all containers stored in the sponsor's safe are locked and keys are retained by authorized credit union staff/volunteers. Spare keys to these containers should be stored under appropriate spare key controls at the main office. Based on the burglary resistant quality of the sponsor's safe, no more than 2000 pounds should be stored in the sponsor's safe during non business hours. As an aside, check with the sponsor to determine what if any coverage is provided should there be a burglary or mysterious disappearance loss.

Safe Alarm - Extortion

The money safe you have provides excellent burglary protection for the currency you're storing during non-business hours. From a burglary perspective a safe alarm is not needed. However, considering you have a robbery alarm with a reporting circuit to the police, adding a door contact on the money safe and wiring it separate from other alarms would give you one added level of protection against someone forcing staff to open the safe. The cost for this added benefit might be very small.

Recommendation: Consider adding a door contact to your money safe the next time you upgrade your alarm system. Controlling who has a shunt key to this safe alarm will help discourage an extortion attempt.

Window Covering

Window covering can be good and bad. Set a goal to provide as much view of the lobby area as possible day and night and a controlled view of the manager's office during business hours. Allowing the public to see into the lobby helps discourage robbery while limiting a view into the manager's office during the day also discourages a potential robber.

Recommendation: Provide a clear view into the lobby by removing any unnecessary decals and all window' covering both day and night. Open the drape in the managers office and place a motion light (activated by movement in the area) on the safe. Ask guards to be alert to any light on in the manager's office during non-business hours. Note there is a suspended ceiling in the manager's office that might lead to other mall tenants. The open drapes and motion light will help detect anyone entering the manager's office via the suspended ceiling.

Money Safe

It appears that over 1 million dollars has been stored at this office during non-business hours. The currency is stored in the safe encased in concrete located in a concrete room with a rate of rise fire door. The concern is that the safe may or may not have a re-lock device in the combination. If not, the burglar could easily punch the combination with hand tools to gain entry.

Recommendation: Consult with your lock and safe provider to evaluate if a re-lock device is built into the door of the money safe. If not, have one installed. If a re-lock can not be installed, I recommend you limit overnight currency storage to 1 million dollars. As an added security feature, consider installing a door contact on the rate of rise fire door. Considering you already have an alarm reporting system to the police, the added door contact should be a low cost and simple security addition.

Hinge Pin Protection

The hinge pins on the rate of rise fire door leading to the money safe are exposed and could be removed to gain entry.

Recommendation: I recommend the hinges should either be spot welded so they can't be removed or be replaced buy hinges that have anchored pins. A lock professional can help implement this recommendation.

ROBBERY ANALYSIS RECOMMENDATIONS

Vault Area

The vault was custom built for the purposes of the previous occupants of the premises. Whilst inspecting the vault it was not apparent whether it was air tight or not. This makes staff/volunteers vulnerable if locked inside by thieves.

Recommendation: Conduct tests to verify whether vault is airtight, if so provides means of communication to outside, intercom or telephone extension may suffice. Do not be the one to find out the hard way.

Panic Alarms: Switches to operate a panic alarm are situated within the teller area, this is good practice. However It was stated they are of the audible time which if operated at time of a robbery may exacerbate the situation to extreme violence.

Recommendation: While a robbery alarm system may not be needed at this time, a warning system such as a light in another room controlled by a switch in the credit union to warn others of a robbery in progress might work. An intercom similar to a "baby alarm" might also work.

Defendable Zone: The teller area is separated from members and possible intruders by the counter which is high and deep enough to deter vaulting and the secure door. However it was not made clear during the visit whether staff/volunteers were aware of the concept of a defendable zone or trained as to what to expect/do at the time of a robbery

Recommendation: Ensure robbery training of staff/volunteers takes place on an annual basis explaining the risks and controls available before, during and after a robbery. This can be provided as part of the free value added service of the CUNA Mutual Group Risk Manager

Banking

The banking book showed two cash deposits during 2002 in excess of the bond coverage. Such amounts are vulnerable to theft or pretend thefts by person banking.

Recommendation: Banking should always be in accordance with the Fidelity Bond coverage of one person one thousand, two persons up to five thousand and an armoured car thereafter.

Robbery – Collection Points

During our visit to the Thompson Road Collection Point, we discussed a number of office layout changes that will help safeguard against both robbery and a mysterious disappearance of cash. For example, volunteers now have limited control over access to their work area making them vulnerable to a fast hit robbery or a grab and run thief.

Recommendation: Create a "defensible" zone at each collection point. Apply the following safeguards at the Finnigan Street collection point and at other collection points.

Controlled Workspace: It is very difficult to control access into the room used by the volunteers at the Finnigan Street collection point. This exposes them to a sense of being out of control as well as a grab and run type theft.

Recommendation: High, wide and deep counters are usually used to separate teller and cash handling areas from the lobby or public access areas. Locked doors and gates are usually used to control access to areas where currency is handled. At the Finnigan Street collection point, the entry door could be cut into a half door and converted to a counter so members would stand outside the room to conduct business. Considering this might not be possible, I recommend the desk be turned so as to establish a controlled area behind the desk for volunteers. Moving furniture now stored in this room would also create a larger controlled working space for volunteers.

Queue lines: At the Finnigan Street collection point, members to include children in the area come in and out of the room at will.

Recommendation: Queue lines might help alert members when they are entering a cash handling and controlled area. Consider something as simple as a rope across the door and a policy that restricts the room to credit union business only.

Cash Box and Cash Handling: While we were at the Finnigan office cash was on the desk and visible from outside the office. This creates an attractive target for a grab and run thief.

Recommendation: The cash box and cash be positioned behind the desk so as to prevent it being seen from outside the room. I further recommend either the desk be equipped with a locked drawer for cash or the cash box be chained to the desk to discourage the grab and run thief. For example, attach an eye bolt to the box and a chain to the desk so during office hours the box can be anchored with a pad lock to the desk. A bike lock through the cash box handle and around the desk leg might also work

Fisheye Peephole in Door: Volunteer now opens the door to allow one member at a time into the office. The concern is, they must open the door to determine who's knocking. This makes them vulnerable to a planned robbery.

Recommendation: Install a fisheye peephole in the entry door so they can determine who's outside the room before opening the door. If in doubt, they should take precautions such as securing all cash before opening the door or calling for assistance.

Robbery Training: **We did not have time during the visit to evaluate staff training relative to robbery or violence in the workplace. Robbery is a growing risk area for all credit union and especially for cash handling collection points.**

Recommendation: **All credit union staff should receive robbery training at least annually. Please call if I can assist you in your staff training effort.**

Bailout/escape Routes: The Finnigan Street collection point office does have an alternative bailout or escape route from the office. This is an excellent life safety feature for staff and should be provided at all credit union offices and collection points. Often staff is not aware or do not consider the benefits of bailout or escape routes.

Recommendation: Discuss this life safety feature and it's recommended use at all robbery-training sessions.

Warning Lights: The Finnigan Street collection point does not have a robbery alarm system or way of warning others of a robbery in progress. This creates the possibility that someone might walk in on a robbery in progress and thereby escalating the event into a violent situation.

Recommendation: While a robbery alarm system may not be needed at this time, a warning system such as a light in another room controlled by a switch in the credit union to warn others of a robbery in progress might work. An intercom similar to a "baby alarm" might also work.

Transportation of Cash **Volunteers from the Finnigan Street collection point now transport cash to the post office at a set time following an established route. This makes them predictable and therefore a more attractive robbery targets.**

Recommendation: **Volunteers should be instructed to, as much as possible, vary the time, route and persons transporting cash. They should also carry the cash concealed, in a locked vehicle when possible and always be aware of alternative bailout/escape routes. Using a cab periodically, especially when transporting larger amounts, should be encouraged as it introduces a third person into the transportation process.**

Robbery Training

Thank you for the opportunity to conduct robbery training at your main office. I noted during the analysis that such training is needed at all offices.

Recommendation: I recommend you consult with your CMG Risk Management Specialists. They can help you with your training needs. Set a goal to conduct such training at least every three months. Include all your guard services and local police in training. It is very important for all credit union staff, guards, and responding law enforcement to know what everyone is and will do before, during and after a robbery. Develop written procedures for your staff, the guards, and local law enforcement.

Post Robbery Trauma Training

Much can be done to assist robbery victims after a robbery.

Recommendation: As part of robbery training, include victim assistance training. For example encourage "non-judgmental" attitudes, victims to talk or vent. Help them deal with their guilt, fear, and sense of being out of control. Alert your Risk Management Specialist at CMG as soon as possible after a robbery.

Written Robbery Response Procedures

I compliment your use of armed and unarmed, uniformed and plain-cloths guards, and robbery alarm systems reporting to local police at each of your offices. Staff at each office indicated a general understanding of the guard's duties, practices, and procedures. Knowing exactly what guards and local law enforcement do and how they will respond to a robbery will help your staff feel more secure, more in control, and more prepared for robbery.

Requirement: In addition to robbery response training sessions that involve all credit union staff, guards, and local law enforcement, work with the guards and local law enforcement to create written guard duties and robbery response procedures. This will ensure that even though guards and employees may change, the quality of the response and their need to focus on life safety concerns will be the same at all locations.

Height Markers

There are no height markers at the exit from the lobby at any of your offices. Such markers will help robbery victims better judge the height of robbers leaving the lobby.

Recommendation: Install height markers at all lobby exits in all offices. Height markers are not only a good tool to use during a robbery, they offer a constant reminder and effective robbery response training tool for your staff. They also offer a deterrent to robbery as they send a message to the potential robber that your staff has been trained and they are ready.

Currency at Teller Stations

I discussed the currency exposure now at teller stations at each office. It appears your staff is making a good effort to conduct cash flow analysis and limit the exposure to only what's needed. I offer my compliments to your front line staff and operations managers.

Recommendation: Continue to reinforce the need for an on-going cash flow analysis both by operations managers and individual tellers. The goal is to limit currency as much as possible on the front lines. Make a discussion of "cash flow analysis" part of your on-going robbery training and awareness program. Constantly remind the frontline staff to limit their currency to only what's needed to provide good member service.

Spreading Teller Currency

I discussed the need to spread frontline currency between at least two locked containers at each teller station. For the most part tellers at each office are doing that. A few however suggested they monitor the cash flow so closely that they only keep what is actually needed.

Recommendation: There is nothing wrong with limiting the primary drawer to only what's needed and keeping all excess currency locked in a safe away from the counter. However, when staff change locations, they may not be able to judge their cash flow needs and excess currency will usually accumulate on the front lines. I recommend you make it a standard at all offices that front line tellers will use two locked drawers or containers to spread their front line currency exposure. At some offices tellers have two locked drawers and at others there is a locked drawer and locked tray. All help spread the exposure. Spreading front line currency both reduces your loss from a fast hit robbery and sends a message to the robbers that staff is well trained. The practice itself creates a deterrent to robbery.

Bait Money

I did not cover this in my 2001 report, however, I noted that "bait money" is not being used at any office. Bait money is money you can identify as coming from your credit union after a robbery.

Recommendation: I recommend you keep bait money in each teller drawer and in any change fund on premise. Simply record the denomination, bank of issue, serial numbers, etc of a number of bills so if they land in the hands of a robber, you'll be positioned to identify the currency as that coming from your credit union.

Dress for Success

Robbers are attracted to anything of value during the robbery. Expensive jewelry, personal credit cards and currency all make employees an attractive added target during a robbery.

Recommendation: Establish an employee dress code that discourages expensive jewelry or the carrying of personal property such as unnecessary currency or personal credit cards. This will better safeguard your employee's valuable personal property as well as reduce their attraction to the robber during an actual robbery.

Vault Door Re-lock Device

There is some doubt as to whether or not a "re-lock" device is built in to the currency vault door. The re-lock device does what it says, it re-locks the door if the burglar attempt a punch job on the combination.

Requirement: Consult with your lock company and have them confirm there is a re-lock device in this vault door. If not, have one installed. An alternative recommendation would be to purchase a TL-15 rated money safe for currency, member collateral, and other valuable property storage.

Defendable Zones

At all offices, it's important to establish defendable zones where employees can go, lock themselves in and summon police. As part of your "what to do during a robbery" training, identify defendable zones and develop a plan for employees to follow during any violent act on premises.

Requirement: At each office instruct guards to identify areas to which employees can retreat during a robbery or other violent act on premise. The area or "defendable zone" should have a lock on the door so employees can lock themselves in as well as a peep holes in doors so employees can see what's going on outside the room. Also, provide a telephone in the zone to call the police. The telephones in the defendable zone should not light extension lights on phones in the teller area. Guards should develop a signal to warn employees of a violent person on premise and instruct them how to reach the zone. Once employees are secure, guards should take planned action to deal with the violence.

Alarm Warning Lights

I did not confirm whether or not warning lights were located in the break room.

Recommendation: Use the same very good approach to alarm warning lights you used at the main office and install alarm warning lights both in the break area and managers office. A light in the manager's office will be especially important if you move the CCTV monitor. The goal is to alert staff in the break room to a robbery in progress so they don't inadvertently walk in and frighten the robber.

Pre-numbered Cash Receipt Vouchers

Volunteers at the collection point update pass books or issue not numbered receipt to the member. There is no audit trail to safeguard against withholding or lapping of receipts

Recommendation: **Volunteers/staff at all collection points and especially door-to-door collections should issue pre-numbered cash receipt vouchers. Each time cash is collected, the member should be given a completed cash receipt voucher, issued in numerical sequence and initialed by the volunteer/staff person. If an error is made when filling out the voucher, it should be marked "void" and retained for accountability. Periodically, the vouchers should be audited to confirm they are being used and agree with cash receipts.**

Bank Reconciliation

At the time of visit the bank deposit book was unavailable to be inspected and therefore bank reconciliation verification not verified. A bank reconciliation is an important risk management tool to ensure monies are correctly and timely deposited to avoid use of Credit Union funds to be used even temporarily by staff/volunteers

Recommendation: **A bank reconciliation should be conducted on a regular basis as a Credit Union grows the time period between a bank reconciliation should be shortened even to a daily basis.**

Sammy Stamps

An excellent marketing tool to encourage junior member and parents to join the Credit Union. As each stamp is equivalent to 20pence a financial risk is evident as each roll of stamps is equivalent to two thousand pounds. Whilst on premises it was apparent no control of numbers of stamps stored was in place thereby exposing Credit Union to potential loss.

Recommendation: **Secure all full rolls of stamps are stored in the safe within the vault on the premises. Issue a set amount of stamps, say 100, on each collection day to be accounted for at close of business.**

Pre-numbered Cash Receipt Vouchers

Volunteers at the collection point update pass books or issue not numbered receipt to the member. There is no audit trail to safeguard against withholding or lapping of receipts

Recommendation: **Volunteers/staff at all collection points and in your future mobile branch should be given a controlled supply of duplicate pre-numbered cash receipt vouchers. Each time cash is collected, the member should be given a completed cash receipt voucher, issued in numerical sequence and initialed by the volunteer/staff person. If an error is made when filling out the voucher, it should be marked "void" and retained for accountability.**

Periodically, the vouchers should be audited to confirm they are being used and agree with cash receipts

Non-Cash Transactions

The internal controls, supervisory committee and internal auditor are all good examples of risk management. The practice of moving money between accounts within the system is a clear way of embezzling funds from a Credit Union and usually is not detected until a substantial amount of money has been stolen.

Recommendation: **The internal auditor or supervisory committee to monitor non-cash transactions on a regular basis especially involving staff, volunteers and family accounts.**

Dormant Accounts

The procedure of holding dormant accounts responsible to a member of staff is a good risk management control. Again these accounts are easily transferred without notice and provide a clear way of embezzling funds.

Recommendation: **Dormant accounts to form part of an analysis by supervisory committee and internal audit thereby preserving the integrity of the staff member responsible.**

Passwords

As in 1999 I noted passwords are not set to automatically force individuals to change them. Because Internet and hacker criminals are getting sophisticated, it's important to maintain tight password controls. Your plan at this time is to have them expire every six months. This according to the experts is too long a period to go without a forced change.

Requirement: I recommend you set them to expire no more than every 90 days. Instruct your management team to monitor this area and strive to set automatic changes every 30 days.

Currency Counting Machine

The currency counting machine is now in the teller area in clear view of anyone in the lobby. This creates an attractive target and motivation for a would-be robber.

Recommendation: The counting machine should be moved to the back office where currency can be counted out of sight.

FIDELITY ANALYSIS

We'll be adding standard answers in this section.

OFFICE SAFETY ANALYSIS RECOMMENDATIONS

We'll be adding standard answers in this seciton

Section IV

Great Britain 300
Application & Bond

*** *The next 32 pages can be used for training purposes but will be replaced with the application and bond forms specific to Great Britain!*

I think the following application is the same but the bond might be different because of endorsements!

Section VI starts about page 49

CUNA MUTUAL INSURANCE SOCIETY

CUNA MUTUAL GROUP Bond Insurance Application/Renewal

ATTACH FINANCIAL STATEMENT AS AT DECEMBER 31, 1999 TO THIS FORM

SECTION 1

Name of Credit Union:_____

Current (Physical Location) Address of Credit Union:

_____

Mailing Address for Credit Union:

_____

Telephone (_____)_____Fax: (_____) _____Hours of Operation:

_____

Number of salaried employees: Full-time _____ Part-time_____

(Over 40 hrs/week) (Under 40 hrs/week)

Number of branch office locations: _____ (A branch office is defined as any credit union facility where business is transacted with credit union members at least 40 hours per week)

Please copy and complete a separate form for each branch office (Sections 1 & 2 only)

SECTION 2

Physical Security: A safe is a free standing container (UL rated TL-15, TL-30 etc.) Indicate safe rating from metal tag on safe. A vault is a walk-in room (ISO-5R, 6R, ASTM Type I, II, and III, UL-Class I, II, III, etc,) Indicate the vault rating from metal tag on vault. If there is no label to identify your safe/vault, measure the thickness of solid steel in the door and thickness of reinforced concrete in the walls, ceiling, floor, and doorframe. If your credit union does not have one of the above, please advise what type of currency storage receptacle is used:

_____

_____

_____

#1 - Safe/Vault Rating: _____Cash Stored:

_____ #2- Safe/Vault Rating:

_____ Cash Stored: _____

Alarm Components on safe/vault (check those present): ☐ Door Contact ☐ Heat Sensor ☐ Sound Detector ☐ None

Describe the line security (e.g. Manufacturer, Mode #, UL rated , DC, Coded, Interrogate/Response, etc)

_____

_____

_____

Does the alarm protect each safe/vault? Explain:

_____

If the Credit Union does not have the above security features describe what features are present:

_____

_____

_____

Maximum cash transported? _____ (Do not include traveler cheques) Check the method of transporting cash used:

☐ One or more credit union employees ☐ Credit union employee (s) plus two armed escorts

☐ Credit union employee (s) plus one armed escort ☐ Armoured car service ☐ Other (explain)_____

_____

_____

Maximum Cash on premises $ _____

Are any firearms kept on the Credit Union premises? ☐ Yes ☐ No If "Yes," please explain purpose:

SECTION 3

What types of Loans are made by your Credit Union:

Consumer Loan $ _____ 1st Mortgage $ _____ 2nd Mortgage and/or Equity $_____
Business/Commercial $ _____ Agriculture $ _____ Other $ _____

Does the Board of Directors have a written policy on investments (e.g. type, maturity?) ☐ Yes ☐ No

SECTION 4

Do you offer credit cards? ☐ Yes ☐ No If yes, number of Card Accounts _____

Do you offer debit or ATM cards? ☐ Yes ☐ No If yes, number of card accounts _____

NOTE: Please complete the following information for each ATM the Credit Union owns or is responsible for. In addition to the address, please indicate if the ATM location is a Credit Union office, shopping mall, parking lot, etc. Please describe installation by indicating, through the wall, lobby, drive -up, kiosk etc.
MANUFACTURER'S NAME, Model Number, Physical location (Address) and amount of currency stored:
1)_____
)_____
3)_____
4)_____
5)_____

Complete the following for ATM's:

Is the ATM alarmed? ☐ Yes ☐ No If yes indicate components present: ☐ Door Contact ☐ Heat Sensor ☐ Lining or Lacing

Reporting Line Security:
Manufacturer_____

To who does alarm report?
_____

Describe method of cash transportation and replenishment for all ATM's:

Maximum distance cash is transported: _____ How often:_____

Transported by armored car? ☐ Armed Guards? ☐ Employees?

Brief description of transportation and replenishing procedures:
_____
_____
_____
_____
_____
_____

Hours of operation that ATM is available for member use:
_____

SECTION 5 – AUDIT PROCEDURE

(a) Is there an annual audit by an independent chartered accountant and/or auditing firm? ___ ☐ Yes ☐ No
(b) If "Yes", is it a complete audit made in accordance with generally accepted auditing standards and so certified? ☐ Yes No ☐ ?
(c) If the answer to (b) is "No", explain the scope of the chartered accountant/auditing firm examination:
_____
_____

If you had any special audits, please include copy of the management letter.

_____

(d) Is the audit report rendered directly to the Board of Directors? _____ Yes No

(e) Name and location of chartered accountant and/or auditing firm:

_____

(f) Date of completion of the last audit by chartered accountant and/or auditing firm:_____

(g) Is there a continuous internal audit by an Internal Audit Department? Yes No

(h) If "Yes" are monthly reports rendered directly to the Board of Directors? Yes No

Is a controlled, positive member account verification conducted annually on 100% of your member share and loan accounts? Yes No

PLEASE ATTACH A COPY OF THE MANAGEMENT LETTER (FROM AUDITORS) WITH THEIR FINDINGS AND RECOMMENDATIONS.

PLEASE ATTACH A COPY OF THE BOARD OF DIRECTORS' ANSWER TO THE MANAGEMENT LETTER

SECTION 6 - INTERNAL CONTROLS (OTHER THAN AUDIT PROCEDURES)

(a) Do you require annual vacations of at least two consecutive weeks for all officers and employees Yes No

If "No," explain:

_____

Is there a formal, planned program requiring the rotation of duties of key personnel, Without prior notice thereof?

_____ Yes No

If "No." explain

_____

_____

(b) Is there a formal, planned program requiring segregation of duties so that no single transaction

and be fully controlled from origination to posting by one person?_____ Yes No

Credit unions face the growing risks of burglary, robbery, forgery and fraud. The following self-assessment questions will help your evaluate existing internal and audit controls now in place. Answer yes, no, or not applicable. Please comment on any “no” answers.

Burglary	Yes	No	NA
1. Are safes and vaults locked during non-business hours?			
2. When safe/vault combinations are written down, are they protected?			
3. If shunt keys/codes are used, are any left on-premise unprotected?			
4. Do you consider lighting in your security program?			
5. Are burglar-resistant locks used on all exterior doors except where prohibited by local fire codes?			
6. Does an access key/code/card control program exist?			

A. Robbery	N/A	NoRec	Rec
1. If Armored Car is used, do they provide insurance at least equal to the			

maximum amount transported?

2. Is currency concealed when transported (note easily recognized).
3. Is a list of check in the deposit kept at the credit union to reconstruct a lost deposit in transit to the bank?
4. Is your Robbery Alarm silent on premise so as not to alert robbers when it's activated?
5. Is the Robbery Alarm tested at least twice a year?
6. Camera
   Lobby
   Drive-Up
7. Do you use Armed Guards?
8. Do Bullet-Resistive Barriers separate your teller and lobby areas?
9. Is your Walk-Up/Drive-Up equipped with Bullet-Resistive Barriers?
10. Do tellers conduct cash flow analysis so as to keep currency at the teller counter to a reasonable minimum?
11. Is currency at each teller stations separated into two individually locked containers to reduce the loss from grab and run robbery?
12. Has staff been trained as to what to do before, during, and after a robbery?
13. Are access controls divided to discourage extortion?
14. Is the counter high and wide enough to discourage vaulting?
15. Is the counter high and wide enough to discourage vaulting?
16. Are height markers used near each exit?
17. Are queue lines used to control lobby traffic?
18. Are sufficient alarm actuators located throughout the credit union?
19. If appropriate, are warning lights used?
20. Are firearms on-premise?

Fraud and Forgery	Yes	No	N/A
1. Are currency deliveries verified by two or more persons acting jointly?			
2. Are signed receipts, initialed logs, or some similar audit trail used each time currency changes hands?			
3. Is access to cash items controlled: Central change fund/Vault cash? Common cash drawer? Travelers checks? Overnight storage?			
4. Are drawers/trays locked when tellers leave the counter?			
5. Are these adequately controlled at all times: Keys? Spare keys? Vault/Safe Keys/Combinations?			
6. Do tellers cash their own or family member checks?			
7. Do employees conduct transactions on their own or family member accounts?			
8. Are surprise cash item counts conducted at least quarterly?			
9. Do surprise counts include all cash items?			
10. Are checks restrictively endorsed in a timely manner?			
11. Are supervisory override controls used?			
12. Is there a supervisory override printout?			
13. If supervisory override controls are used, are transactions: Reviewed regularly? By someone without override authority?			
14. To the degree possible, are safeguards to access the computer used?			
15. Does the credit union have written policies on all expenses and reimbursement procedures?			
16. Does the individual who approves expense accounts also have general ledger posting authority?			
17. Prior to payment, are corporate expenses, including credit card charges, reviewed and approved by the next higher level of supervision?			
18. Is suspense account activity reviewed by someone other than the person performing the transactions?			
19. Is the overdraft suspense account reviewed by someone other than the overdraft processor?			
20. Are dormant and inactive account properly monitored?			
21. Are adequate controls established for signature machines and signature plates: During business hours? Non-business hours? Access to checks?			

23. Are mail deposits processed under dual control?			
24. Are deposits in night and lobby depositories: Processed under dual control? Protected by key/combination?			
25. Is a log/record documented for each opening of the night depository?			
26. Does the credit union have a written overdraft policy?			
27. Does the credit union have a written share draft policy?			
28. Does the credit union have a procedure to deal with funds availability?			
29. Does the credit union have a written fraud policy?			
30. Does the credit union use the bondability verification service?			
Other Internal Control Concerns:			

Names and titles of Principal Officers:

_____ _____

MANAGER OR TREASURER (Please type or print)

FINANCIAL OFFICER (Please type or print)

Completed by _____ _____

SIGNATURE

DATE

Great Britain Fidelity Bond 300

June 16, 2002

1. **A Focus on Bond Coverage:**
- Employee or Director Dishonesty, On Premises (Burglary & Robbery), In Transit, Forgery and Alteration, Counterfeit Currency, Audit Expense, Business Credit Cards, Employee's Property, Travel Advance, Members Property
2. **Second Focus on Exclusions and on What Might Be Requested:**
- Plastic Card (PIN), Fraudulent Deposits, Electronic Crimes, Liability Coverage, DVE/PI/EPL

Group

CIS
Co-operative Insurance

Bonding Scheme Policy

We (the Co-operative Insurance Society) agree with you (the Association of British Credit Unions) that, subject to the Declarations, Definitions, Exclusions General Agreements and Conditions of this Policy, we will provide the insurances set out in the Insuring Clauses and in any Endorsements specified as operative to each **Member** in respect of events occurring during the Period of Insurance shown in the Declarations and any further period for which we may accept a renewal premium.

Claims under this Policy will be met from our Share Capital, General Business Fund and General Reserve only.

Signed on our behalf.

Chief General Manager

Declarations

Policyholder Association of British Credit Unions Limited
Address Holyoake House, Hanover Street, Manchester M60 OAS
Renewable on 1st October

Policy Number FY 5526404
Agency 1.39.335

Period of Insurance from 12.01 a.m. on 1st October 2001 to 12.01 a.m. on 1st October 2002

The Limits of Liability shown below represent our liability under each Insuring Clause, the limit applicable to each **Member** being set out in their Bonding Certificate.

Aggregate Value of share subscriptions and other deposits received and not paid		Limits of Liability (any one claim) for Insuring Clauses A to G and M	
Exceeding	Not Exceeding	Minimum Limit	Maximum Limit
£	£	£	£
-	20,000	5,000	10,000
20,000	50,000	10,000	20,000
50,000	100,000	20,000	30,000
100,000	200,000	30,000	60,000
200,000	400,000	60,000	90,000
400,000	600,000	90,000	120,000
600,000	800,000	120,000	150,000
800,000	1,000,000	150,000	225,000
1,000,000	1,500,000	225,000	300,000
1,500,000	2,000,000	300,000	450,000
2,000,000	3,000,000	450,000	600,000
3,000,000	4,000,000	600,000	750,000
4,000,000	5,000,000	750,000	900,000
5,000,000	6,000,000	900,000	1,050,000
6,000,000	7,000,000	1,050,000	1,200,000
7,000,000	8,000,000	1,200,000	1,350,000
8,000,000	9,000,000	1,350,000	1,500,000
9,000,000	10,000,000	1,500,000	1,650,000
10,000,000	11,000,000	1,650,000	1,800,000
11,000,000	12,000,000	1,800,000	1,950,000
12,000,000	13,000,000	1,950,000	2,100,000
13,000,000	14,000,000	2,100,000	2,250,000
14,000,000	15,000,000	2,250,000	2,400,000
15,000,000	16,000,000	2,400,000	2,550,000
16,000,000	17,000,000	2,550,000	2,700,000
17,000,000	18,000,000	2,700,000	2,850,000
18,000,000	19,000,000	2,850,000	3,000,000
19,000,000	20,000,000	3,000,000	3,150,000
20,000,000	21,000,000	3,150,000	3,300,000

The Limit of Liability for Insuring Clause H is 50% of the amount of the loss payable under Insuring Clause A, subject to a maximum of £1,000, but this amount may be increased in increments of £1,000 to a total of £5,000 (or a total of £10,000 for a further single £5,000 increment) where the extra premium has been paid. Credit unions whose policy limit exceeds £1,000,000 have a further option to purchase an additional £15,000 (in £5,000 increments) up to a total of £25,000.

The Limit of Liability for Insuring Clauses I, J, K and L is £6,400 in respect of any one occurrence.

The limit (any one claim) under Insuring Clause B is 50% of the credit union's Limit of Liability, subject to a maximum of £100,000.

The limit (any one claim) under Insuring Clause C is (a) £1,000 whilst in the custody of one **Employee** (b) £5,000 whilst in the custody of a minimum of two **Employee**'s, and (c) equivalent to the limit payable under Insuring Clause B whilst being carried by an **Armoured Car** vehicle company, subject to a maximum of £100,000.

The Aggregate Limit of Liability for any one year combining all Insuring Clauses is equal to 5 times the Limit of Liability any one claim.

A deductible of one per cent of the **Member**'s Limit of Liability (any one claim) will apply to each claim, subject to a maximum of £2,500.

Definitions

Each of the following words and expressions is given a specific meaning which applies whenever it appears in **bold type** in this Policy.

1. Armoured Car

An **Armoured Car** carrier is an entity which for hire provides secured transportation of valuables by means of specifically designed and constructed bullet-resistant **Armoured Car** vehicles and **Armoured Car** guards. **Armoured Car** vehicles will be specifically designed for the transportation and security of **Covered Property** while in transit. Such vehicles will be designed to deter robbery, fire, accident and other perils using appropriate metallic materials providing armour against such perils. Such vehicles will also be appropriately appointed with communications and deterrent security features. Individuals operating such **Armoured Car** vehicles will be professionally licensed, certified, bonded and trained while under the employment and supervision of the **Armoured Car** vehicle company.

2. Automated Teller Machine

Automated Teller Machine means an electronic mechanical device which requires the use of an access card or personal identification number (PIN), or both, to disburse currency or accept deposits.

3. Cash Letter

Cash Letter means a letter:

a. Containing share drafts, cheques, drafts, promissory notes and like items that the **Member** has accepted for deposit, payment, collection or exchanged for cash, together with a detailed listing of same; and

b. Which is sent by the **Member** for deposit, payment, collection or exchange for cash.

4. Certified Securities

Certified Securities means shares participations or other interests in property of or enterprises of the issuer, or obligations of the issuer, which are:

a. Represented by an instrument issued in bearer or registered form; and

b. Of a type commonly dealt in on securities exchanges or markets or commonly recognised in any area in which it is issued or dealt in as a medium for investment; and

c. Either one of a class or series or by its items divisible into a class or series of shares, participations, interests or obligations.

5. Computer Programmes

Computer Programmes means sets of related electronic instructions that:

a. Direct the operations and functions of a computer or equipment connected to it; and

b. Enable the computer or equipment to receive, process, store or send **Electronic Data**.

6. Computer Systems

Computer System means computers, with their related components by which data are electronically collected, transmitted, processed, stored and retrieved, including:

a. Storage components; and

b. **Computer Programmes;** and

c. Terminal devices; and

d. Related data communication networks.

Definitions

7. Covered

Covered Property means the following items in which the Member has have

Property — **a financial interest or which are held by the Member in any capacity:**

a. Currency, coins, bank notes; or

b. Cheques, drafts or share drafts; or

c. Original mortgages, documents of title, evidences of debt, security agreements, money orders, time deposits or Certified Securities; or

d. Precious metals, jewellery, gemstones, tickets, stamps or coupons.

8. Director — **Director** means a person elected or appointed to the **Member**'s Board of Directors according to the **Member**'s charter or bylaws and the laws under which the charter is issued.

9. Electronic Data — **Electronic Data** means facts or information converted to a form usable in a **Computer System**.

10. Employee

1. **Employee** means any of the following persons when performing work for the **Member** under the **Member**'s immediate direction and control:

    a. Persons to whom the **Member** pay a wage or salary; or

    b. Persons provided by an employment service; or

    c. Persons serving on the **Member**'s committee appointed or elected by the **Member**'s Board of Directors or by the **Member**'s membership in accordance with the **Member**'s bylaws or by written resolution of the **Member**'s Board of Directors; or

    d. The **Member**'s credit union volunteers, except for **Directors** acting as **Directors;** or

    e. Persons who are **Directors** but are acting in the capacity of an **Employee**, as defined here.

2. **Employee** also means:

    a. Persons legally appointed to act on the **Member**'s behalf as trustee, receiver or liquidator of the credit union; or

    b. Employees of a credit union consolidated or merged with the **Member** prior to the effective date of this Policy.

3. For Employee or Director Dishonesty Coverage only, **Employee** also means:

    a. Persons retained by the **Member** to act on their behalf to collect the unpaid balance of the **Member**'s delinquent **Loan** account; or

    b. Persons retained by the **Member** to perform services as the processor of the **Member**'s cheques or drafts; or

    c. Retained accountants and their staff only while performing accounting services for the **Member**; or

    d. Retained lawyers and their staff only while performing legal services for the **Member**.

    e.

Definitions

10. Employee (continued)

4. Unless specifically listed in paragraphs 1, 2 or 3 above, **Employee** does not mean:

   a. Independent contractors; or

   b. Agents, meaning a person authorised by the **Member** to act for them; or

   c. Brokers; or

   d. Consultants; or

   e. Persons acting on behalf of a **Service Centre** including those who might otherwise be the **Member**'s **Employee**, or

   f. The **Member**'s credit or debit card processor.

11. Environment

Environment means:

a. Any person; or

b. Any man-made object or feature; or

c. Any animals, crops or vegetation; or

d. Any land, bodies of water, underground water or water table supplies, air and any other feature of the earth or its atmosphere, whether or not altered, developed or cultivated and whether or not owned, controlled or occupied by the **Member**.

12. Forgery

Forgery means the unauthorised and unratified signing of the name of another natural person with the intent to deceive. A mechanically reproduced facsimile signature is treated the same as a handwritten signature.

Forgery does not mean a person signing his or her own name, with or without authority, in any capacity, for any purpose.

13. Instruments

Instrument means an original: mortgage, document of title, promissory note, security agreement, money order, time deposit, **Certificated Securities**, bond coupon, interim receipt for a security, assignment of mortgage, share draft, cheque, bill of exchange, withdrawal order, letter of credit, acceptance, passbook held as collateral, warehouse receipt or bill of lading.

14. Lawsuit

Lawsuit means a civil court action.

15. Loan

Loan means:

a. Any extension of credit by the **Member**; or

b. Any transaction creating a creditor relationship in the **Member**'s favour; or

c. Any transaction by which the **Member** assumes an existing creditor relationship.

16. Member

Member means a credit union registered with the Registrar of Friendly Societies and which holds a valid Bonding Certificate issued by you.

17. Pollutants

Pollutants means:

a. Noise, solid, semisolid, liquid, gaseous or thermal irritants or contaminants; or

b. Smoke, vapour, soot, fume, acid, alkali, chemical, biological or other causative agents or materials; or

Definitions

17. Pollutants (continued)

c. Electromagnetic or ionising radiation and energy, genetically engineered materials, teratogenic, carcinogenic and mutagenic materials and waste. Waste includes any material to be disposed of, recycled, reconditioned or

reclaimed; or

d. Other irritants, contaminants or controlled or prohibited substance.

18. Pollution or Contamination

Pollution or Contamination means any conditions that:

a. Are unclean, unsafe, damaging, injurious, or unhealthy; and

b. Result directly or indirectly from the presence of **Pollutants**, whether permanent or transient in any **Environment**.

19. Premises

Premises means:

a. Any of the Member's offices; or

b. Offices of any financial institutions used by the Member for safekeeping; or

c. The Member's retained lawyers' office.

Premises do not include a Service Centre's place of business.

20. Service Centre

Service Centre means a business entity that:

a. Is not a credit union; and

b. Has a place of business at which members of two or more credit unions may interact with a person to transact business with the members' respective credit unions.

To be a **Service Centre** the business entity must offer share deposit and share withdrawal transactions among its services.

A **Service Centre**'s place of business may be located at a credit union's place of business.

21. Single Loss

Single Loss means all loss or losses covered under this Policy, including court costs and lawyers' fees if recoverable from, or paid by, us under the General Agreements of this Policy, resulting from:

a. Any one act or omission, or series of related acts or omissions, on the part of any person, whenever occurring; or

b. All acts or omissions, whether related or not, on the part of any person or in which such person is implicated, whenever occurring; or

c. Any one casualty or event not specified in a. or b. above.

22. Theft

Theft means the taking of property:

a. Without the **Member**'s consent and with the intent to deprive the **Member** of the property; or
b. By false pretence and with the intent to deprive the **Member** of the property

Definitions

22. Theft (continued)

Theft does not mean the taking of property by means of **Forgery** or alteration.

23. Uncertificated Securities

Uncertificated Securities means shares, participations or other interests in property of or enterprises of the issuer, or obligations of the issuer, which are:

a. Not represented by an instrument and the transfer of which is registered

upon books maintained for that purpose by or on behalf of the issuer; and

b. Of a type commonly dealt in on securities exchanges or markets; and

c. Either one of a class or series or by its terms divisible into a class or series of shares, participations, interests or obligations.

Insuring Clauses

A. Employee or Director Dishonesty

We will pay the **Member** for their loss resulting directly from dishonest acts committed by an **Employee** or **Director**, acting alone or in collusion with others.

Such dishonest acts must be committed by the **Employee** or **Director** with the manifest intent to:

a. Cause the **Member** to sustain such loss; and

b. Obtain financial benefit for the Employee or Director, or for any other person or entity.

Financial benefit does not include any benefits earned in the course of employment including salaries, commissions, fees, bonuses, promotions, awards, profit sharing, business entertainment or pensions.

B. On Premises

1. We will pay the **Member** for their loss of **Covered Property** resulting directly from **Theft** committed:

   a. By a person physically present on the **Member**'s **Premises**; and

   b. While the **Covered Property** is on the **Member**'s **Premises**.

2. We will pay the **Member** for loss of or damage to the property listed below resulting directly from a **Theft** or attempted **Theft** on the **Member**'s **Premises:**

   a. Offices; or

   b. Furnishings; or

   c. Fixtures; or

   d. Supplies; or

   e. Paper books; or

   f. Paper records; or

   g. Equipment.

   Coverage is provided only if the **Member** owns or is legally liable for the above property. Coverage is not provided if the loss or damage results directly or indirectly from fire in connection with the **Theft** or attempted **Theft**.

3. We will pay the **Member** for their loss of **Covered Property** resulting directly from its mysterious unexplainable disappearance, misplacement, damage or destruction while on the **Member**'s **Premises**.

C. In Transit

We will pay the **Member** for their loss of **Covered Property** resulting directly from its **Theft**, mysterious unexplainable disappearance, misplacement, damage or destruction while in transit and within the custody of:

a. An **Employee** acting as a single messenger for amounts not exceeding £1,000. Such amounts may be maintained in the **Employee**'s residence over a period of no more than one night followed by a business day and or up to three nights if each night is followed by a non-business day

b. Two or more **Employee**'s for amounts not exceeding £5,000

c. An **Armoured Car** vehicle company for amounts exceeding £5,000 up to the limit payable under Insuring Clause B, subject to a maximum of £100,000

Insuring Clauses

C. In Transit (continued)

Transit begins immediately upon receipt of the **Covered Property** by such **Employee** or other natural person the **Member** has selected to act as their messenger, or such armoured motor vehicle company, and ends immediately upon delivery at the destination of deposit.

D. Extortion, Kidnap And Ransom

We will pay the **Member** for their loss of **Covered Property** surrendered away from the **Member**'s **Premises** because a threat has been made to the **Member**, the **Member**'s **Employee** or **Director:**

a. To physically harm someone; or

b. To damage the **Member**'s personal or real property; or

c. To sell or disclose the **Member**'s security information; or

d. To introduce or make active a computer virus in the **Member**'s **Computer system**.

We will also pay the **Member** for their continued payments of salaries and benefits to an **Employee** or **Director** while detained against his/her will, up to a maximum of two years from the first day of such detention.

E. Counterfeit Currency

We will pay the **Member** for their loss resulting directly from their acceptance of counterfeit currency or money orders.

F. Cash Letter

1. We will pay the **Member** for the loss, in whole or in part, of the **Member**'s **Cash Letter** resulting directly from its **Theft**, mysterious unexplainable disappearance, misplacement, damage or destruction while in transit by any commercially reasonable means the **Member** authorises for the purpose of deposit, payment, collection or exchange for cash.

   The **Member** must make every reasonable effort to identify depositors and obtain duplicates of the items contained in the **Cash Letter**. We will pay the **Member** for the reasonable costs they incur to reduce a covered **Cash Letter** loss.

2. Coverage will not be afforded under paragraph 1., above, unless the **Member** has a procedure in place to make and retain a photographic or electronic image record of the **Cash Letter**.

   The **Member** will be considered to have complied with their procedure if the photographic or electronic image record is not available because:

   a. There was mechanical failure of the equipment; or

   b. The film was damaged or destroyed; or

   c. The film is not readable; or

   d. The **Member**'s **Employee** made an error or omission in complying with the **Member**'s procedure.

G. Electronic Crime

1. We will pay the **Member** for their loss resulting directly from fraudulent:

   a. Entry of, or change to, **Electronic Data** or **Computer Programmes** in the **Member**'s **Computer System** or the **Member**'s data processors' **Computer system**: or

   b. Communications through electronic, telefacsimile or telephonic means received, sent or purportedly sent by the **Member**, provided that commercially reasonable identification procedures were followed and such communications received by the **Member** were

G. Electronic Crime

either recorded or logged by them.

Such fraudulent entry, change or communication must cause the addition, deletion, change, debit or credit of an account or data field.

2. We will pay the **Member** for their loss resulting directly from the malicious destruction of or damage to the **Member**'s **Electronic Data** or **Computer Programmes** by a computer virus or other malicious use of **Computer Programmes**.

Our liability for loss of or damage to **Electronic Data** or **Computer Programmes** is limited to the cost of duplication of such **Electronic Data** or **Computer Programmes** from other **Electronic Data** or **Computer Programmes** the **Member** furnishes.

If the **Computer Programmes** cannot be duplicated from other **Computer Programmes**, the amount we will pay is limited to the reasonable cost incurred to restore the **Computer Programmes** to substantially the previous level of operational capability. Such costs may include:

a. Computer time; or

b. Computer programmers; or

c. Consultants; or

d. Other technical specialists.

H. Audit Expense

1. We will pay the **Member** for the necessary and reasonable fees and expenses the **Member** pays for a special audit of their records. Such special audit must establish a valid and collectible loss under Employee or Director Dishonesty Coverage or, if purchased, Faithful Performance Endorsement.

   Such special audit must be performed by a recognised provider of auditing services. **Employees** salaries and other expenses are not covered without our prior consent.

2. We will not pay under paragraph 1., above for:

   a. A routine or periodic audit even though it may result in the establishment of a covered loss; or

   b. Correcting, modernising or otherwise preparing the **Member**'s books and records after they have discovered a covered loss.

3. For fees and expenses covered under paragraph 1., above, we will pay the **Member** the lesser of:

   a. The Single Loss Limit of Liability for Audit Expense Coverage shown on the Declarations subject to the applicable Annual Aggregate Limit of Liability; or

   b. The special audit fees and expenses the **Member** paid; or

   c. 50% of the covered loss under Employee or Director Dishonesty Coverage or, if purchased, Faithful Performance Endorsement.

I. Travel Advances

We will pay the **Member** for their loss of funds they have advanced to an employee or director for their business travel expenses when the loss results directly from its **Theft**, damage or destruction of those funds.

J. Business Credit Cards

We will pay the **Member** for their loss resulting directly from the unauthorised use of a lost, altered, stolen or counterfeited credit card issued to the **Member** for use by their **Employees** or **Directors** solely for the payment of their expenses related to business or travel for them.

K. Employees' Property

We will pay the **Member** for an **Employees', Directors'**, and volunteers' loss of property stolen or damaged by a person committing a robbery or burglary:

a. On the **Member**'s **Premises;** or

b. In the **Member**'s car park, drive or pavement immediately adjacent to the **Member**'s credit union office; or

c. At an **Automated Teller Machine** owned or operated by the **Member**; or

d. While the **Employee** is transporting the **Member**'s **Covered Property** for the **Member**; or

e. At a **Service Centre** authorised to conduct transactions on the **Member**'s behalf.

L. Members' Property

We will pay the **Member** for their members' loss of property stolen or damaged by a person committing a robbery or burglary:

a. On the **Member**'s **Premises;** or

b. In the **Member**'s car park, drive or pavement immediately adjacent to the **Member**'s credit union office; or

c. At an **Automated Teller Machine** owned or operated by the **Member**; or

d. At a **Service Centre** authorised to conduct transactions on the **Member**'s behalf.

M. Fraudulent Deposit and Forgery or Alteration

We will pay the **Member** for their loss resulting directly from a person depositing or exchanging for cash with the **Member** a cheque, draft or other item that is ultimately not paid, providing that:

a. The person intended to commit a fraud by depositing or exchanging for cash the cheque or draft, and

b. The **Member** made payment or extended credit against the cheque or draft.

We will pay the **Member** for their loss resulting directly from the **Forgery** or alteration of an **Instrument**.

Exclusions

We will not pay for:

1. Automated Teller Machines

Any loss resulting directly or indirectly from burglary, robbery or mysterious unexplainable disappearance, damage or destruction or **Covered Property** contained within **Automated Teller Machines**, except as may be covered under:

a. Employee or Director Dishonesty Coverage; or

b. On Premises Coverage.

2. Computer Programmes

Any loss resulting directly or indirectly from **Theft** of **Computer Programmes** and operating systems as loaded on **Computer Systems** and is no longer supported by the manufacturer or cannot be reasonably replicated.

3. Data Recognition

Any loss under Insuring Clauses A, B, C, K, L and M and any applicable endorsements, directly or indirectly caused by or consisting of or arising from the failure of any computer, data processing equipment or media, microchip, integrated circuit or similar device or any computer software, whether occurring before, during or after the year 2000

a. correctly to recognise any date as its true calendar date

b. to capture save or retain, and/or correctly to manipulate, interpret or process any data or information or command or instruction as a result of treating any date otherwise than as its true calendar date

c. to capture save retain or correctly to process any data as a result of the operation of any command which has been programmed into any computer software, being a command which causes the loss of data or the inability to capture save retain or correctly to process such data on or after any date.

4. Depository Institution Failure

Any loss resulting directly or indirectly from the failure of a financial or depository institution, or its receiver or liquidator, to pay or deliver the **Member**'s property or property for which the **Member** is legally liable, except as may be covered under:

a. Employee or Director Dishonesty Coverage; or

b. On Premises coverage.

5. Directors

Any loss resulting directly or indirectly from acts or omissions of a **Director**, except as may be covered under:

a. Employee or Director Dishonesty Coverage; or

b. Otherwise covered under this Policy as a loss resulting directly from misplacement, mysterious unexplainable disappearance or destruction.

6. Employees

Any loss resulting directly or indirectly from acts or omissions of **Employees**, except as may be covered under:

a. Employee or Director Dishonesty Coverage; or

b. Faithful Performance Endorsement; or

c. Otherwise covered under this Policy as a loss resulting directly from misplacement, mysterious unexplainable disappearance or destruction.

Exclusions

7. Employment Practices

Any loss resulting directly or indirectly from employment practices, policies, acts or omissions including, but not limited to:

a. Refusal to hire or promote; or

b. Termination of employment; or

c. Coercion, demotion, evaluation, reassignment, discipline, defamation, harassment, humiliation or discrimination.

8. Fines, Penalties And Restitution

Any loss resulting directly or indirectly from a civil or criminal fine or penalty, order of forfeiture or order of restitution.

9. Forgery

Any loss resulting directly or indirectly from **Forgery** or alteration, except as may be covered under:

a. Employee or Director Dishonesty Coverage; or

b. Business Credit Cards Coverage; or

c. Forgery or Alteration Coverage.

10. Indirect Loss

Any indirect or consequential loss, including, but not limited to:

a. Loss of use of property; or

b. Diminution of value of property; or

c. Earnings or interest not realised by the **Member**, whether past, present or future, earned or unearned.

11. Insufficient Funds/Closed Account

Any loss resulting directly or indirectly from any payment made or withdrawal from a **Member**'s account that was closed or had insufficient funds at the time of the payment or withdrawal, except as may be covered under:

a. Employee or Director Dishonesty Coverage; or

b. Faithful Performance Endorsement.

12. Investments

Any loss resulting directly or indirectly from investments, investment transactions or trading of any kind or nature, whether authorised or unauthorised, except as may be covered under:

a. Employee or Director Dishonesty Coverage; or

b. Forgery or Alteration Coverage.

13. Lawyers' Fees

Any lawyers' fees, court costs or other legal expenses, except as may be covered under Lawyers' Fees and Court Costs General Agreement.

14. Loans

Any loss resulting directly or indirectly from the complete or partial non-payment of or default on a **Loan** or transaction in the nature of or amounting to a **Loan**, whether such **Loan** or transaction was obtained in good faith or through trick, artifice, fraud or false pretences, except as may be covered under:

a. Employee or Director Dishonesty Coverage; or

b. Faithful Performance Endorsement; or

c. Forgery or Alteration Coverage.

Exclusions

15. Mail/Carrier For Hire

Any loss resulting directly or indirectly from loss of or damage to property while in the mail or within the custody of a carrier for hire other than an **Armoured Car** vehicle company, except as may be covered under:

a. Employee or Director Dishonesty Coverage; or
b. Cash Letter Coverage

16. Mechanical Breakdown

Any loss resulting directly or indirectly from mechanical breakdown or failure to function properly of any equipment, **Computer System**, **Automated Teller Machine** or other machine.

17. Missing Endorsement

Any loss resulting directly or indirectly from the **Member**'s acceptance for deposit or for exchange for cash of an item which is missing an endorsement except as may be covered under Employee or Director Dishonesty Coverage.

18. Non-Compensatory Damages

Any damages of any type for which the **Member** is legally liable, except compensatory damages, but not multiples of compensatory damages, arising directly or indirectly from a loss covered under this Policy.

19. Nuclear

Any loss resulting directly or indirectly from nuclear reaction, radiation or radioactive contamination.

20. Out Of Balance

Any loss evidenced only by an unreconciled difference or out of balance condition in the **Member**'s financial records.

21. Plastic Card/PIN

Any loss resulting directly or indirectly from the use of a personal identification number (PIN) to access an **Automated Teller Machine**, or of a plastic or other type of card to effect a transaction, except as may be covered under:

a. Employee or Director Dishonesty Coverage; or
b. Business Credit Cards Coverage; or
c. Fraudulent Deposit Coverage; or
d. Forgery or Alteration Coverage.

22. Pollution

Any loss resulting directly or indirectly from:

a. The **Pollution or Contamination** of any **Environment** by **Pollutants** or seepage of **Pollutants** that are introduced at any time, anywhere, in any way; or

b. The actual, alleged or threatened discharge, dispersal, release or escape of **Pollutants**; or

c. Any costs, or other loss or damage arising out of such **Pollution or Contamination** or seepage including, but not limited to cleaning up, remedying, testing, monitoring, containing, treating detoxifying, and neutralising such contamination, seepage, or **Pollutants**, even if caused by a governmental direction or request; or

d. Payment for the investigation or defence of any loss, injury or damage, or any cost, fine, penalty, expense, claim or **Lawsuit** related to any of the above.

Exclusions

23. Property Owned by Others

Any loss of property owned by others, unless the **Member** makes a record that includes its description and value within three days of receipt, except as may be covered under:

a. Employee or Director Dishonesty Coverage; or

b. Employees' Property Coverage; or

c. Members' Property Coverage.

24. Safe Depository

Any loss of members' property held by the **Member**, as safe depository, contained in safe deposit boxes or vaults, except as may be covered under Employee or Director Dishonesty Coverage.

25. Service Centre

Any loss of property:

a. Owned by a **Service Centre**, or

b. Held by a **Service Centre** in any capacity.

26. Shortages

Any loss evidenced only by a shortage in a teller's daily transaction record.

27. Stop Payment

Any loss resulting directly or indirectly from a payment over a valid stop payment order, except as may be covered under Employee or Director Dishonesty Coverage.

28. Telephone Toll Charges

Any loss resulting directly or indirectly from telephone toll charges, except as may be covered under Employee or Director Dishonesty Coverage.

29. Uncollected Funds

Any loss resulting directly or indirectly from a cheque, draft or other item that is not finally paid for any reason, except as may be covered under:

a. Employee or Director Dishonesty Coverage; or

b. Fraudulent Deposit Coverage; or

c. Forgery or Alteration Coverage.

30. War

Any loss resulting directly or indirectly from war, including undeclared or civil war, warlike action by a military force, insurrection, revolution, usurped power or action taken by governmental authority in hindering or defending against any of these.

31. Wear And Tear

Any loss resulting directly or indirectly from mechanical failure, faulty construction, error in design, latent defect, wear and tear, gradual deterioration or electrical disturbance.

General Agreements

1. The Member Warranty

A statement made by or on behalf of the **Member**, whether contained in the application or otherwise, is a warranty that the statement is true to the best of the knowledge and belief of the person making the statement.

2. Additional Offices

1. This Policy automatically provides coverage for additional offices the **Member** establishes during any Annual Policy Period other than by consolidation or merger with, or purchase or acquisition of assets or liabilities of, another institution.

2. Such additional offices are automatically covered from the date the **Member** establishes them, and no notice to us or payment of additional premium for the remainder of such Annual Policy Period is required.

3. Additional Employees, Consolidation, Merger or Purchase of Assets

1. If the **Member** consolidates or merges with, or purchase or acquire assets or liabilities of, another institution during any Annual Policy Period, then except as provided in paragraph 2., below, this Policy does not automatically cover loss which:

   a. Has occurred or will occur in offices or premises the **Member** acquires as a result of such consolidation, merger, purchase or acquisition; or

   b. Has been or will be caused by employees or directors of such institution; or

   c. Has arisen or will arise out of the assets or liabilities the **Member** acquires as a result of such consolidation, merger, purchase or acquisition.

2. This Policy will automatically provide coverage for loss described in paragraphs 1.a., 1.b., 1.c. above if:

   a. Such loss results directly from acts or occurrences that take place during the period commencing on the effective date of such consolidation, merger, purchase or acquisition and expiring not later than 90 days thereafter; and

   b. Such loss is discovered within the period for the discovery of loss under this Policy; and

   c. The **Member** pays to us the additional premium due for such coverage.

3. The **Member** may obtain coverage under this Policy for loss described in paragraphs 1.a., 1.b. and 1.c. above without the limitations in paragraph 2. above if:

   a. The **Member** gives us written notice of the proposed consolidation, merger, purchase or acquisition before its effective date; and

   b. We, at our option, gives our written consent to extend the coverage provided under this Policy to such additional offices or premises, employees, directors and other exposures; and

   c. The **Member** pays us the additional premium due for such coverage.

4. Lawyers' Fees And Court Costs

1. Notice of lawsuits brought against the **Member**.

   The **Member** must notify us immediately of any **Lawsuit** brought against them to determine their liability for any loss, claim or damage which, if established, would constitute a collectible loss under this Policy. The **Member** must also immediately furnish to us copies of the summons, complaint or other papers regarding the **Lawsuit**.

2. Our election to defend

   We may, at our sole option, elect to conduct the defence of a **Lawsuit**, in whole or in part, in which claims or causes of action are asserted which, if established, would constitute a collectable loss under this Policy. Should we so elect:

   a. We will select lawyers of our choice to conduct the defence in the **Member**'s name; and

   b. The **Member** will co-operate with us and our chosen lawyers in the **Member** defence; and

   c. The following will be covered losses under this Policy, subject to the applicable Single Loss Limit of Liability, Annual Aggregate Limit of Liability, and deductible in effect during the Annual Policy Period in which Discovery of Loss occurs:

      1) Any judgement against the **Member** on a claim or cause of action constituting a collectible loss under this Policy; and

      2) Any settlement in which we participate to the extent of its payment; and

      3) All lawyers' fees, costs and expenses incurred by us in the defence.

3. If we do not elect to defend

   a. If we do not elect to defend a **Lawsuit** under paragraph 2. above, then the **Member** will be responsible for conducting and paying for their own defence. Neither a judgement against the **Member** nor a settlement by the **Member** will determine the existence or amount of coverage under this Policy. If such judgement or settlement, in whole or in part, is found to establish a covered and collectible loss under this Policy, then subject to the applicable Single Loss Limit of Liability, Annual Aggregate Limit of Liability, and deductible in effect during the Annual Policy Period in which Discovery of Loss occurs, we will pay:

      1) The amount of the judgement or settlement that constitutes a covered and collectible loss under this Policy; and

      2) The reasonable lawyers' fees, costs and expenses incurred by the **Member** in the defence of only those claims or causes of action upon which that portion of the judgement or settlement is based.

   b. If we do not defend a **Lawsuit** under paragraph 2. above, then during the **Lawsuit** the **Member** does not have to comply with the their duties following Discovery of Loss or Notice of Discovery of Loss in this Policy. However, upon the entry of any judgement or the consummation of any settlement, the **Member** must then comply with all conditions of this Policy that apply following Discovery of Loss.

1. Annual Policy Period

An Annual Policy Period is the 12 month period beginning on the effective date of this Policy, and each 12 month period thereafter beginning on the anniversary of that effective date until cancelled. This Policy continues in force until cancelled, subject to all other Conditions.

We will determine the premium using the rates we have in effect at the beginning of each Annual Policy Period.

2. Annual Aggregate Limit of Liability

The Annual Aggregate Limit of Liability shown in Section 1. of the Declarations in effect during any one Annual Policy Period is the maximum amount that we will be liable to pay for all loss or losses discovered during that Annual Policy Period under all coverages listed in Section 1. For any endorsement or sub-part shown in Section 2. of the Declarations in effect during any one Annual Policy Period, the Annual Aggregate Limit of Liability separately shown is the maximum amount that we will be liable to pay for all loss or losses discovered during that Annual Policy Period under that endorsement or sub-part.

Any applicable Annual Aggregate Limit of Liability will be reduced by all payments made under the applicable coverages, endorsements of sub-part of this Policy during any one Annual Policy Period, including amounts recoverable from, or paid by, us under Lawyers' Fees and Court Costs General Agreement. If a loss of **Certificated Securities** is settled through use of a lost instrument bond, the face amount of such bond will not exceed the remaining balance of the Annual Aggregate Limit of Liability for the applicable coverages, endorsements or sub-part, but such loss will not reduce the applicable Annual Aggregate Limit of Liability until such time as we are required to make a payment under such lost instrument bond. The amount of such payment will reduce the applicable Annual Aggregate Limit of Liability in the Annual Policy Period in which such payment is made.

When our payments reach the applicable Annual Aggregate Limit of Liability, all coverage for that Annual Policy Period under Section 1 of the Declarations, or under the particular endorsement of sub-part listed in Section 2 of the Declarations, as the case may be, will be exhausted. Upon the exhaustion of an Annual Aggregate Limit of Liability:

a. We will have no further liability for loss or losses discovered during that Annual Policy Period, whether or not previously reported to us, under the applicable coverages, endorsement or sub-part; and

b. The total premium for such coverages, endorsements or sub-part for that Annual Policy Period will be considered earned; and

c. If we have elected to defend the **Member** under Paragraph 2. of Lawyers' Fees And Court Costs General Agreement with respect to a potential loss under such coverages, endorsements or sub-part we will have no further obligation to defend them. Upon the **Member**'s receipt of notice from us of the exhaustion of the Annual Aggregate Limit of Liability, the **Member** will assume all responsibility for their defence at their own cost.

Annual Aggregate Limits of Liability will not be increased or reinstated by amounts recovered from third parties.

3. Single Loss Limit of Liability

Subject to the applicable Annual Aggregate Limit of Liability, the maximum amount we will be liable to pay for a **Single Loss** is the applicable Single Loss Limit of Liability shown on the Declarations in effect when such **Single Loss** is discovered.

If we have elected to defend the **Member** under paragraph 2. of Lawyers' Fees And Court Costs General Agreement with respect to a potential loss, we will have no further obligation to defend the **Member** upon the exhaustion of the applicable Single Loss Limit of Liability. Upon the **Member**'s receipt of notice from us of the exhaustion of the Single Loss Limit of Liability, the **Member** will assume all responsibility for their defence at the their own cost.

4. Non-Stacking Of Limits

Regardless of the number of Annual Policy Periods this Policy is in effect, we will not:

a. Be responsible for more than the applicable Annual Aggregate Limit of Liability shown on the Declarations then in effect for all loss or losses discovered during any one Annual Policy Period; or

b. Pay more for a **Single Loss** than the applicable Single Loss Limit of Liability shown on the Declarations in effect at the time that such **Single Loss** is discovered.

5. Single Loss Deductible

We will be liable to pay the **Member** only that part of a **Single Loss** that exceeds the applicable Single Loss Deductible shown on the Declarations, subject to the applicable Single Loss Limit of Liability and Annual Aggregate Limit of Liability.

6. Other Insurance

The coverage provided under this Policy will be excess over any other valid and collectible insurance, indemnity of bond coverage which applies or would have applied in the absence of this Policy.

7. Termination Or Limitation Of Coverage For Employee Or Director

1. This Policy's coverage for an **Employee** or **Director** terminates immediately when one of the **Member**'s **Directors**, officers or supervisory staff not in collusion with such person learns of:

   a. Any dishonest or fraudulent act committed by such **Employee** or **Director** at any time, whether or not related to the **Member**'s activities or of the type covered under this Policy; or

   b. Any termination of bond coverage for such **Employee** or **Director** by any bonding company, for which coverage was not reinstated.

2. We at our sole option may terminate coverage for an **Employee** or **Director**. Such termination will be effective 15 days after receipt by the **Member**.

3. Termination of coverage for an **Employee** or **Director** under paragraphs 1. or 2. above terminates our liability for any loss resulting from any act or omission by that **Employee** or **Director** occurring after the effective date of such termination.

4. We at our sole option may issue an endorsement applying a separate deductible or limit of liability, of other such measures as we deem necessary, for acts or omissions or any **Employee** or **Director**. Such endorsement will be effective 15 days after receipt by the **Member**.

8. Discovery Of Loss

This Policy applies to loss discovered by the **Member** while this Policy is in effect. Discovery occurs when the **Member** first becomes aware of facts which would cause a reasonable person to assume that a loss of a type covered under this Policy has been or will be incurred, regardless of when the act or acts causing or contributing to such loss occurred. The exact amount or details of loss may not be known at the time of discovery.

Discovery also occurs when the **Member** receives notice of an actual or potential claim alleging that they are liable to a third party under circumstances which, if true, would constitute a loss under this Policy.

9. Notice Of Discovery Of Loss

The **Member** must send us a written notice at the earliest practicable moment after Discovery of Loss, but not to exceed 30 days after such discovery, without regard to amount or whether the loss appears to exceed any deductible.

10. The Member Duties In Event Of A Loss

The **Member** must do the following in event of a loss:

a. Within 180 days after notice of discovery of loss to us, submit a complete, sworn Proof of Loss. It must include the necessary explanation and documentation to prove the cause of the loss, the amount of the loss and the identity of the persons, if known, who caused the loss. The sworn Proof of Loss must be signed by the President or Chairperson of the Board of Directors and the signature must be notarised; and

b. Take all reasonable measures to minimise the loss after learning of it, including collection or other efforts; and

c. Give us reasonable access to the **Member**'s property, books, records and operations that are relevant to the loss; and

d. Notify the appropriate law enforcement authorities if a criminal law may have been broken; and

e. Permit us to question the **Member**'s **Directors** and **Employees** at reasonable times. The questioning may be under oath, and they may be required to sign their statements; and

f. Immediately send us any legal papers or notices received concerning the loss; and

g. Co-operate with us in all matters pertaining to this loss.

11. Loss Payment

We will make payment within 30 days after we reach agreement with the **Member** on the amount payable under this Policy.

12. Valuation Of Property

We will determine the value of certain property as follows:

a. Foreign Currency. The value of foreign currency will be calculated at the rate of exchange on the day the loss was discovered.

b. Securities. The value of **Certificated Securities** or **Uncertificated Securities** will be the market value as of the close of business on the day the loss was discovered. If no market value is readily available and the valuation cannot be agreed upon, the market value will be determined by arbitration. We may, at our option, provide a lost instrument bond to secure replacement of a certificate. The face amount of the lost instrument bond will not exceed the remaining balance of the applicable Single Loss Limit of Liability or Annual Aggregate Limit of Liability.

12. Valuation Of Property (continued)

c. Paper Books and Paper Records. The value of paper books and paper records will be the cost of blank paper books and blank paper records plus the cost of labour for the actual transcription of data. The **Member** must furnish the data to be transcribed.

d. Other Property. The value of offices, furnishings, fixtures, supplies and equipment will be the lesser of the cost of repair or the cost of replacement with items of like kind and quality without deduction for depreciation.

13. Application Of Realised Earnings In Loan Losses

1. If the **Member** incurs a covered loss resulting from a **Loan**, we will reduce the amount of the their covered loss by the amount of the **Member**'s realised earnings, including interest and fees, on that **Loan**.

2. If the **Member** incurs a covered loss under Employee or Director Dishonesty Coverage resulting from a **Loan**, we will reduce the amount of the **Member**'s covered loss by the amount of the their realised earnings, including interest and fees:

   a. On that **Loan**; and

   b. On any other dishonest **Loans** originated or caused by the same dishonest **Employee** or **Director**.

14. Legal Action Against Us

Legal proceedings against us to recover loss under this Policy:

a. Cannot be brought before the expiration of 60 days after the original Proof of Loss; and

b. Must be brought within 2 years after Discovery of Loss.

15. Rights To Recover From Others

If the **Member** has the right to recover all or part of any loss that we have made payment under this Policy, we will be subrogated to those rights and those rights will be assigned to us. The **Member** must do everything reasonably necessary to secure and protect those rights. The **Member** must not do anything to impair those rights.

16. Recovered Property

Any recoveries less the cost of obtaining the recoveries will be distributed as follows:

a. First to the **Member**, until they are reimbursed for any part of their applicable loss not paid by us solely because it exceeds any limit of liability and any deductible;

b. Then to us, until we are reimbursed for our payment made to the **Member**;

c. Then to the **Member**, until they are reimbursed for that part of the loss equal to any deductible;

d. Then to the **Member**, for any uncovered loss.

17. Cancellation

Cancellation is effective:

a. 60 days after the **Member** receives a written notice from us that we have elected to cancel this Policy or any Policy endorsement; or

b. On the date specified in the **Member**'s written notice to us that the **Member** has elected to cancel this Policy or any Policy endorsement, or immediately upon our receipt if no date is specified; or

17. Cancellation (continued)

c. 30 days after a receiver or liquidator is appointed for the **Member**; or

d. Immediately when the **Member** merges into, or is taken over by, another credit union of financial institution; or

e. Immediately when the **Member** fails to pay premium when due.

When required, we will give written notice to the **Member**'s supervisory authority of cancellation of this Policy.

Our only obligation after cancellation of this Policy or any endorsement is to return to the **Member** the pro rate unearned premium for the remainder of the Annual Policy Period during which the cancellation becomes effective, unless the premium has already been considered earned due to exhaustion of the applicable Annual Aggregate Limit of Liability.

18. Discovery Extension

An additional period of time not exceeding 18 months in which to discover a loss the **Member** sustained before the effective date of cancellation of this entire Policy may be obtained from us. An additional premium determined by us must be paid for such additional period. Such additional period must be requested by the **Member** in writing sent to us before cancellation becomes effective. A loss discovered during the extension period is subject to the applicable Single Loss Limit of Liability, Annual Aggregate Limit of Liability, and deductible in effect during the Annual Policy Period in which the cancellation occurred. Upon receipt of such written request, we will issue an appropriate Discovery Extension Endorsement. Such additional period of time will terminate on the effective date of any insurance obtained by the **Member** or the **Member**'s successor that provides any of the types of coverages afford by this Policy. We will refund an unearned premium.

19. Audit And Inspection

1. We may examine and audit the **Member**'s books, records and **Premises** and interview **Employees** and **Directors** as they relate to this Policy at any time.

2. We have the right, but are not obligated to:

   a. Make inspections and surveys at any time; or

   b. Give the **Member** reports on the conditions that we find; or

   c. Recommend changes.

3. Any inspections, surveys, reports or recommendations relate only to insurability and the premiums to be charged and are performed only for our own benefit and use.

4. We do not:

   a. Make any warranties to the **Member** regarding these inspections, surveys or reports; or

   b. Make safety inspections; or

   c. Undertake to perform the duty of any person or organisation to provide for the health or safety of workers or the public; or

   d. Assume any duties to the **Member** as a result of its inspections, surveys or reports.

5. This condition also applies to any rating advisory, rate service or similar person or organisation which make insurance inspections, surveys, reports or recommendations on our behalf.

Conditions

20. Conformity With Laws

If any term of this Policy, as written or applied, is found to be invalid under the law of any jurisdiction, then:

a. If permitted under such law, that term will be considered amended only to the extent necessary to conform with such law; and

b. Such invalidity will not affect the validity of that term in any other jurisdiction; and

c. Such invalidity will not affect the validity of any other term of this Policy in that or any other jurisdiction.

21. Modification Of Policy Terms

This Policy contains all the agreements between the **Member** and ourselves concerning the coverage provided. This Policy's terms can be modified only by written endorsement issued by us and made a part of this Policy.

22. Offset Clause

We may collect any balances due from the **Member** by deducting the amount due us from premium to be refunded or claim payments to be made.

23. Non-assignment

1. This Policy may not be assigned by the **Member** without written consent by us.
2. This Policy is solely for the **Member**'s use and benefit.
3. Only the **Member** has the right to make a claim under this Policy.

24. Territory

Coverage under this Policy applies in Great Britain, Northern Ireland, the Isle of Man and the Channel Islands only.

Section V

CMG Risk Management Tools - To be edited in Great Britain

a) Data Sheets (SA, ICA, FA, FD/FA, ATM)
b) Suggested Recommendations/Requirements follow each Data Sheets
c) Suggested Cash Item Storage Guidelines follow the SA Burglary Data Sheets
d) * Hard cover manuals contain data sheets with line by line explanations
e) RMA Cover Letters - Examples
f) RMA Report Example
g) Bond Survey Example
h) Memo to File Format
i) Brochure lists
j) www.cunamutual.com link
k) US Cash Item Guidelines

Security Analysis

Contract #: _____

II. Burglary

A. Cash and Travelers Checks Storage	N/A	NoRec	Rec
Are they stored in adequate containers?			

B. Currency Vault	N/A	NoRec	Rec
1. Is the vault properly alarmed?			
2. Are time locks: Used? Set by two employees?			
3. Are combination locks properly used?			

C. Record Vault	N/A	NoRec	Rec
Are cash items stored within guidelines? Alarm components adequate?			

D. Record Safe	N/A	NoRec	Rec
Are cash items stored within guidelines?			

E. Fire-Resistive Files	N/A	NoRec	Rec
1. Are cash items stored within guidelines?			
2. Are loan files protected?			

F. Money Safes	N/A	NoRec	Rec
1. Is the safe properly alarmed?			
2. Is the location acceptable?			

G. Alarm System	N/A	NoRec	Rec
1. Internal Line Security			
2. External Line Security			
3. Control Cabinet Location			
4. Standby Hours			
5. Alarm Reporting			
6. Perimeter & Area Alarm			
7. Separate Shunt			

I. H.	Additional Burglary Information	N/A	NoRec	Rec
1.	Are safes and vaults locked during nonbusiness hours?			
2.	When safe/vault combinations are written down, are they protected?			
3.	If shunt keys/codes are used, are any left on-premise unprotected?			
4.	Does the credit union consider lighting in its security program?			
5.	Are burglar-resistant locks used on all exterior doors except where prohibited by local fire codes?			
6.	Does an access key/code/card control program exist?			

III. Robbery

A.	Transportation & Security	N/A	NoRec	Rec
1.	Armored Car Insurance Limits			
2.	Employee Cash Transportation Within Limits			
3.	Employee Cash Transportation, Concealment			
4.	Transporting Checks, Filming			
5.	Robbery Alarm			
6.	Camera Lobby Drive-Up			
7.	Armed Guards			
8.	Lobby Bullet-Resistive Barriers			
9.	Walk-Up/Drive-Up Bullet-Resistive Barriers			
10.	Maximum Currency At A Teller Station			
11.	Teller Funds Divided			

B.	Additional Robbery Information	N/A	NoRec	Rec
1.	Has staff been trained as to what to do before, during, and after a robbery?			
2.	Are access controls divided to discourage extortion? Opening procedures? Ambush code?			
3.	Is the counter high and wide enough to discourage vaulting?			
4.	Are there: lockable barriers/doors protecting the teller area? are they locked?			
5.	Are height markers used near each exit?			
6.	Are queue lines used to control lobby traffic?			
7.	Are sufficient alarm actuators located throughout the credit union?			
8.	If appropriate, are warning lights used?			
9.	Is the credit union aware of the "Americans With Disabilities Act"?			
10.	Are firearms on-premise?			

The Risk Management Specialists in Great Britain should develop their own cash item storage guidelines after consulting with CMG personnel in Great Britain and CMG personnel in Madison. I offer the following as a starting point:

Taking into consideration the loss history in Great Britain and the type burglary tools and methods most often used, I recommend Risk Management Specialists working in Great Britain adopt the following as cash item storage guidelines:

Credit union that store more than $500US during non-business hours should provide at least a TL-15 rated money safe. A TL-15 rating usually requires a 1" solid steel body and 1 ½" solid steel door (50,000PSI Steel) equipped with a Group 2 combination lock with a re-lock device.

These guidelines became effective 9-1-99 and are now permanent.

Safe Rating	No Alarm or Substandard Alarm System	a. Low-Grade External Line Security & b. Door Contact, Heat Sensor & Sound Detector	a. High-Grade External Line Security & b. Door Contact, Heat Sensor & Sound Detector
TL-15	$100,000	$200,000	$300,000
TL-15X6	$150,000	$300,000	$450,000
TL-30	$150,000	$300,000	$450,000
TL-30X6	$200,000	$350,000	$500,000
TRTL15X6	$300,000	$750,000	$1,200,000 [1]
TRTL-30	$400,000	$600,000	$900,000 [1]
TRTL30X6	$500,000	$750,000	$1,000,000 [1,2]
Class I, II, or III Currency Vault	$500,000	$750,000	$1,000,000 [1,2]
ATMs, cash dispensing machines level 1 or 2, and TL-15 or better night depositories	$50,000	$75,000	$100,000
UL rating "business hour" (maximum of 2 units per location)	$1,000	$5,000	$15,000

1=These limits, as noted above require high-grade internal line security.
2=Higher limits, up to the bond limit, can result after consultation with an Underwriter.

Security Analysis (SA) – "Burglary"
Recommendations/Requirements to edit in Great Britain

BURGLARY ANALYSIS

Currency Storage

Up to $[Click here and enter amount] in currency and $[Click here and enter amount] in travelers checks are being stored in a [Click here and enter container type] during nonbusiness hours. This container was designed to protect contents against heat and fire.

Recommendation: We recommend you limit the cash items stored on-premise to a combination of $[Click here and enter amount] in cash and travelers checks. Of this total amount, cash should not exceed $[Click here and enter amount]. If these figures are too restrictive, we recommend you purchase an Underwriters Laboratories Inc. (UL) listed TL-15 money safe. This safe will provide adequate protection for up to $200,000 in currency and a reasonable amount of travelers checks.

Vault Alarm

The presence of [Click here and edit]safe deposit boxes, large amounts of currency, and travelers checks during nonbusiness hours presents an attractive target to a professional burglar.

Recommendation: We recommend the following alarm components be installed on the currency vault:

- Audio Accumulator - detects noise resulting from hammering, drilling, etc.
- Heat Detector - detects heat resulting from a torch attack.
- Door Contact - detects unauthorized opening of the vault door.
- High-grade Internal Line Security - protects the alarm reporting line between the vault alarm components and the alarm control panel. The specifications for this line security should equal or exceed Diebold's PLS II, Mosler's ILS, or LeFebure's FLS-1.
- Low-grade External Line Security - protects the alarm reporting line between your credit union and the alarm reporting station. The specifications for this line security should equal or exceed Diebold's Multi-Guard II, Mosler's PAC-A, or LeFebure's PM 3101.
- High-grade External Line Security - protects the alarm reporting line between your credit union and the alarm reporting station. The specifications for this line security should equal or exceed Diebold's Multi-Guard V, Mosler's HLS, or LeFebure's LM 3101.

  An alternative is to use an Underwriters Laboratories Inc. (UL) rated "AA" radio frequency (RF) reporting system or a high-grade cellular system. The specifications for the cellular system can be found in "Cellular Alarm Installation Specifications" (CRM-336).

- Standby Power Supply - the alarm system should be equipped with a “fail-safe” standby reserve power supply which is capable of operating the alarm system for a minimum of 48 hours if electrical power is lost.
- Alarm Shunt - the alarm should be installed with a separate shunt for the vault alarm so that authorized persons will be able to enter the premises without disarming the vault alarm.

Time Lock

The currency vault is equipped with a time lock. This is an important feature designed to prevent access to the vault at unauthorized times. However, this feature is not used and important protection is lost.

Recommendation: We recommend using the vault time lock each day. Two employees should verify the setting just prior to securing the vault at the end of the day. The setting should prevent opening of the vault door until shortly before business hours the next working day.

Time Lock

The currency vault is equipped with a time lock. This is an important feature designed to prevent access to the vault at unauthorized times. However, this feature is not used and important protection is lost.

Recommendation: We recommend using the vault time lock each day. Two employees should verify the setting just prior to securing the vault at the end of the day. The setting should prevent opening of the vault door until shortly before business hours the next working day.

Combination Locks

[No standard recommendation]

Record Vault

Up to $[Click here and enter amount] in currency and $[Click here and enter amount] in travelers checks are being stored in your record vault during nonbusiness hours. This vault was designed to protect contents against heat and fire, and offers limited resistance to forced entry.

Recommendation: We recommend you purchase an Underwriters Laboratories Inc. (UL) listed TL-15 money safe. This safe will provide adequate protection for up to $200,000 in currency and a reasonable amount of travelers checks.

Record Safe

Up to $[Click here and enter amount] in currency and $[Click here and enter amount] in travelers checks are being stored in your record safe during nonbusiness hours. This safe was designed to protect contents against heat and fire, and offers limited resistance to forced entry.

Recommendation: CUNA MUTUAL GROUP guidelines allow you to store up to $10,000 in currency, or up to $20,000 in currency and travelers checks, during nonbusiness hours. If this is too restrictive, excess travelers checks may be stored in a safe deposit box at your bank. Another option would be to purchase an Underwriters Laboratories Inc. (UL) listed TL-15 money safe, which will provide adequate protection for up to $200,000 in currency and a reasonable amount of travelers checks.

Physical Security

As much as $[Click here and enter amount] in travelers checks is stored in your fire-resistive file cabinet during nonbusiness hours. Such a device is designed to provide fire protection and offers limited resistance to forced entry. Therefore, no more than $5,000 in cash should be stored in a fire-resistive file cabinet during nonbusiness hours. Nor should the combined total of cash and travelers checks exceed $15,000. Inadequate security is provided for your level of exposure.

Recommendation: To achieve the guidelines stated above, we recommend storing excess travelers checks in a safe deposit box at the credit union's bank.

Loan Files

Loan files are in a record room that was not constructed to meet fire protection standards. In case of a fire, these documents may be damaged. You may face losses if these documents cannot be saved.

Recommendation: We recommend storing loan files in locations properly protected from fire. At a minimum, they should be in fire-resistive file cabinets with a rating at least equal to Underwriters Laboratories Inc. (UL) rating of 350 degree - one hour.

Safe Alarm

The large amounts of currency (up to $[Click here and enter amount]) and travelers checks stored during nonbusiness hours present an attractive burglary target. Due to current day expertise and available equipment, a professional burglar may be able to defeat your present physical and electronic security.

Recommendation: To provide reasonable protection for the cash items stored during nonbusiness hours, we recommend installing a safe alarm with at least the following components and features:

- Audio Accumulator - detects noise resulting from hammering, drilling, etc.
- Heat Sensor - detects heat resulting from a torch attack.
- Door Contact - detects unauthorized opening of the safe door.
- Low-grade Internal Line Security - protects the alarm reporting line between the safe alarm components and the alarm control panel. The specifications for this line security should equal or exceed Diebold's PLS I, Mosler's ILS, or LeFebure's FLS-1.

- Low-grade External Line Security - protects the alarm reporting line between your credit union and the alarm reporting station. The specifications for this line security should equal or exceed Diebold's Multi-Guard II, Mosler's PAC-A, LeFebure's PM 3101, or "Scan-Alert".
- High-grade External Line Security - protects the alarm reporting line between your credit union and the alarm reporting station. The specifications for this line security should equal or exceed Diebold's Multi-Guard V, Mosler's HLS, or LeFebure's LM 3101.

  An alternative is to use an Underwriters Laboratories Inc. (UL) rated "AA" radio frequency (RF) reporting system or a high-grade cellular system. The specifications for the cellular system can be found in "Cellular Alarm Installation Specifications" (CRM-336).
- Standby Power Supply - the alarm system should be equipped with a "fail-safe" standby reserve power supply which is capable of operating the alarm system for a minimum of 48 hours if electrical power is lost.
- Alarm Shunt - the alarm should be installed with a separate shunt for the safe alarm so that authorized persons will be able to enter the premises without disarming the safe alarm.

Once this recommendation is implemented, the safe and alarm system would be considered adequate security for up to $[Click here and enter amount] in cash and a reasonable amount of travelers checks.

Safe Location

[No standard recommendation]

Internal Line Security

The internal lines of an alarm system run between the alarm control cabinet and the alarm actuators. These can be subject to attack or circumvention. Your system only provides [Click here and type text]-grade internal line security.

Recommendation: We recommend upgrading your alarm system to include a random interrogate/response internal line supervision system equal to Diebold's PLS II or Mosler's ILS. An acceptable alternative is to move the alarm control box inside the vault. The internal lines to the vault alarm would receive the protection of the vault and the alarm system.

External Line Supervision

Your existing external line security is inadequate for the amount of cash which has been as much as $[Click here and enter amount] stored in your currency vault. It is currently connected to a digital dialer which can be circumvented by cutting the phone lines.

Recommendation: We recommend upgrading your alarm system to include high-grade interrogate/response external line supervision that meets the standards for a "AA" certificate from Underwriters Laboratories Inc. (UL). A few examples of such systems are Diebold's Multi-Guard V, Mosler's HLS, LeFebure's LM-3800, and "Scan-Alert".

A preferable option for you may be the use of a cellular phone back-up system to obtain this high-grade system rating. Please refer to “Cellular Alarm Installation Specifications” (CRM-336).

Location of Control Cabinet

[No standard recommendation]

Alarm Standby Power

Your alarm system includes a standby power supply which can provide only [Click here and enter amount] hours of power to the alarm system if electrical power is lost. If a power loss occurred on a weekend or holiday, the system could not provide enough power to extend until employees returned.

Recommendation: We recommend upgrading the standby power supply for your alarm system to one capable of providing at least 48 hours of power to the alarm system if electrical power is lost.

Alarm Reporting

[No standard recommendation]

Building Alarm

Your building does not have any perimeter (door or window contacts) or area (motion detector) alarms. There is no detection of break-in which could result in burglary or vandalism losses.

Recommendation: We recommend installing motion detectors in the building. These devices should be on separate shunt switches to allow building access (for cleaning crew, etc.) without unalarming the vault alarms.

Alarm Shunting Procedure

The shunt key which deactivates the perimeter and area alarm also deactivates the safe/vault alarm system. Anyone who has access to the shunt key, for example a custodian, can deactivate the entire alarm system, making an important safeguard completely ineffective.

Recommendation: We recommend the safe/vault alarm be rekeyed and put on a separate circuit from the perimeter/area alarm. This will allow authorized persons to access the credit union while the safe/vault remains fully protected by the alarm system.

Safe/Vault Lock

[No standard recommendation]

Safe Combination

The combination to your money safe is written down and retained on-premise. If unauthorized persons gained access to the combination, the safe could be opened and you could sustain a loss.

Recommendation: We recommend the combination to your money safe not be retained on-premise during nonbusiness hours. If it is necessary to retain the combination on-premise, it should be coded as something other than a combination, for example a telephone number.

Spare Shunt Keys

The spare alarm shunt keys are being stored in [Click here and enter text] during nonbusiness hours. If the keys are discovered by unauthorized persons during an attempted burglary, the alarm system could be turned off and rendered useless. An attack on the [Click here and enter text] could then commence with no alarm being sent to the reporting station.

Recommendation: We recommend all spare alarm shunt keys remain inside the [Click here and enter text] during nonbusiness hours.

Building Lights

[No standard recommendation]

Door Locks

[No standard recommendation]

Access Program

[No standard recommendation]

We reviewed your exposures to burglary. We have no recommendations in this area.

Security Analysis (SA) – "Robbery"
Recommendations/Requirements to edit in Great Britain

ROBBERY ANALYSIS

Armored Car Service

Your armored car service contract limits the armored car company's liability for your cash shipments to $[Click here and enter amount]. At times, your cash shipments exceed that limit.

Recommendation: We recommend increasing the liability limitation in your armored car service contract to an amount sufficient to cover the full amount of all your cash shipments. In the alternative, you should limit your cash shipments to the amount of liability provided.

Transportation of Cash

Employees are transporting up to $[Click here and enter amount] in cash to the credit union. When transporting cash, a potential for loss exists. This can extend even beyond the amounts transported to include civil liability relating to employee and public safety.

Recommendation: We recommend using the following security guidelines as minimum standards for transporting cash:

- When transporting $50,000 or less, use one or more employees.
- When transporting between $50,000 and $100,000, use one employee and one armed guard.
- When transporting in excess of $100,000, use an armored car service.

Procedure for Transporting Cash

When employees transport cash to and from the bank, it is carried in a bank bag in open view to the public. This offers an open invitation for robbery and exposes employees to potential danger. Every possible effort needs to be taken to protect the employees involved.

Recommendation: We recommend concealing cash transported by employees in a briefcase, envelope, purse, or other device. This will make it less obvious cash is being carried, thereby reducing the exposure to danger.

Cash Letter Transportation

Cash letters are not filmed or photocopied before they are transported to the bank for deposit. If cash letters are lost or stolen while in transit, they may be difficult or costly to reconstruct.

Recommendation: We recommend filming or photocopying all cash letters before they are transported.

Robbery Alarm

There is no robbery alarm on-premise to quickly summon emergency assistance. The lack of a robbery alarm fails to provide sufficient protection for the credit union's assets and employees.

Recommendation: We recommend installing a silent robbery alarm system reporting directly to the police or an alarm company. Actuators should be at each teller station and desks with unobstructed views of the lobby and teller area.

Camera

You do not have cameras in your security system. A photograph of a robber greatly increases the chance of prosecution.

Recommendation: We recommend installing a wide angle 35mm sequence camera over the entrance/exit of your credit union. The camera should be wired into your robbery alarm system. Cameras also serve as robbery deterrents.

Surveillance Camera

You do not have security cameras at your drive-up windows. Cameras help to identify individuals perpetrating fraud and robbery, and they assist in resolving member disputes.

Recommendation: We recommend installing cameras overlooking the drive-up lanes.

Armed Guards

[No standard recommendation]

Lobby Bullet-resistive Barriers

[No standard recommendation]

Walk-up/Drive-up Bullet-resistive Barriers

[No standard recommendation]

Currency at Teller Stations

As much as $[Click here and enter amount] in cash is kept in teller cash drawers during business hours. Teller cash drawers should be monitored to reduce the exposure to loss due to robbery.

Recommendation: We recommend limiting the cash at teller stations to as low a level as possible. Based on your apparent cash needs, we suggest a maximum limit of $[Click here and enter amount].

If it is necessary to retain larger amounts of currency at the teller counter, we recommend dividing the cash at each teller station between two locking drawers. The upper drawer should contain a minimum amount of working cash. Excess cash should be secured in the lower drawer.

Teller Drawers

[No standard recommendation]

Robbery Training

Credit union robberies continue to increase throughout the country. The affect on employees who have suffered from robbery trauma can be devastating. Proper training of robbery situations can help reduce this loss exposure and alleviate trauma and stress.

Recommendation: We recommend you conduct a thorough annual robbery training session involving all employees. Personnel should be trained on methods of reducing robbery exposures and conduct before, during, and after a robbery. Your local law enforcement or FBI may also assist you in robbery training sessions.

Opening Procedures

Opening procedures are not consistent to reduce the possibility of attack on employees. The potential for loss through civil liability for failing to properly protect employees could far exceed that lost in a robbery.

Recommendation: We recommend expanding daily opening procedures that include at least the following elements:

- External Reconnaissance - may be conducted from within an automobile, to examine the building's exterior and grounds for signs of forced entry or suspicious persons.
- Internal Walk-through - to ascertain no intruders are concealed inside the facility.
- All-clear Signal - to advise other arriving employees that it is safe to enter or to serve as a distress signal. Such a signal could consist of opening or closing a window shade, turning a light on or off, etc. The distress signal should cause other employees to leave the area and call the police.

Ambush Code

The digital keypad that disarms the burglary alarm at opening time is not equipped with an ambush code. This could be an important feature if the employee is confronted by a robber and forced to open the credit union.

Recommendation: We recommend expanding your alarm protection to include an ambush code that will allow employees to send a distress signal while appearing to disarm the system.

Counter Height

[No standard recommendation]

Door to Teller Area

There is no barrier between the lobby and the area behind the teller line. If a robbery occurred, the robber would have little difficulty accessing the area behind the teller line, which contains currency, confidential documents, and personnel.

Recommendation: We recommend a door or gate be installed between the lobby and teller area and this door remain locked during business hours.

Door to Teller Area

The door to the teller area is not locked during business hours. Robbers would have little difficulty accessing the area behind the teller line, which contains currency, confidential documents, and personnel.

Recommendation: We recommend the door between the lobby and teller area remain locked during business hours.

Height Markers

You do not have any form of height markers to assist in the description of the robber.

Recommendation: We recommend you add some method of height measurement at the exit to assist in the identification of the robber.

Lobby Queue Lines

[No standard recommendation]

Robbery Alarm Actuators

All actuators for the robbery alarm are at teller stations. In a “takeover” style robbery (when the robber goes behind the counter), tellers are forced away from the actuators. They might not have time to trip the system. A delay in emergency assistance may result.

Recommendation: We recommend installing additional robbery alarm actuators at various workstations located away from the immediate teller counter. These positions should have good visual contact with the teller area.

Alarm Warning Lights

Employees working in areas removed from the lobby and teller area have no way of knowing if the robbery alarm is actuated.

Recommendation: We recommend installing robbery alarm warning lights in the work areas, hallways, etc., not visible from the lobby. Employees should be instructed to stay away from the lobby and teller area when the lights are activated.

Americans with Disabilities Act

Credit union facilities have not been reviewed to ensure they comply with the terms of the Americans with Disabilities Act.

Recommendation: We recommend you discuss the facilities with your attorney to ensure they meet the requirements of the Americans with Disabilities Act.

Firearms

We learned a firearm is kept on-premise. If this weapon injures an employee, member, or even a suspect, it is likely the credit union will be held liable.

Recommendation: We strongly recommend removing all firearms from the premises. The board should establish written policies forbidding firearms on credit union property.

We reviewed your exposures to robbery. We have no recommendations in this area.

Internal Control Analysis

Contract #: _____

	N/A	NoRec	Rec
1. Are currency deliveries verified by two or more persons acting jointly?			
2. Are signed receipts, initialed logs, or some similar audit trail used each time currency changes hands?			
3. Is access to cash items controlled: Central change fund/Vault cash? Common cash drawer? Travelers checks? Overnight storage?			
4. Are drawers/trays locked when tellers leave the counter?			
5. Are these adequately controlled at all times: Keys? Spare keys? Vault/Safe Keys/Combinations?			
6. Do tellers cash their own or family member checks?			
7. Do employees conduct transactions on their own or family member accounts?			
8. Are surprise cash item counts conducted at least quarterly?			
9. Do surprise counts include all cash items?			
10. Are checks restrictively endorsed in a timely manner?			
11. Are supervisory override controls used?			
12. Is there a supervisory override printout?			
13. If supervisory override controls are used, are transactions: Reviewed regularly? By someone without override authority?			
14. To the degree possible, are safeguards to access the computer used?			
15. Does the credit union have written policies on all expenses and reimbursement procedures?			
16. Does the individual who approves expense accounts also have general ledger posting authority?			
17. Prior to payment, are corporate expenses, including credit card charges, reviewed and approved by the next higher level of supervision?			
18. Is suspense account activity reviewed by someone other than the person performing the transactions?			

	N/A	NoRec	Rec
19. Is the overdraft suspense account reviewed by someone other than the overdraft processor?			

20. Are dormant and inactive account properly monitored?			
21. Are adequate controls established for signature machines and signature plates: During business hours? Nonbusiness hours? Access to checks?			
22. Are checking accounts reconciled: By someone without signing authority? On a timely basis?			
23. Are mail deposits processed under dual control?			
24. Are deposits in night and lobby depositories: Processed under dual control? Protected by key/combination?			
25. Is a log/record documented for each opening of the night depository?			
26. Does the credit union have a written overdraft policy?			
27. Does the credit union have a written share draft policy?			
28. Does the credit union have a procedure to deal with funds availability?			
29. Does the credit union have a written fraud policy?			
30. Does the credit union use the bondability verification service?			
Other Internal Control Concerns:			

Internal Control Analysis (SA)

RECOMMENDATIONS/REQUIREMENTS TO EDIT IN GREAT BRITAIN

Currency Verification

Only one employee verifies currency received from the bank[Click here and remove unneeded text]armored car service. This procedure provides the opportunity for misappropriation of these funds while claiming a shortage in the shipment. In the event of a legitimate shortage, the employee could be wrongly accused.

Recommendation: We recommend when currency is received, it should be verified immediately by two employees acting jointly.

Transfer of Currency

When tellers receive additional currency from the vault cash, a signed, dated receipt is not generated. A receipt provides an excellent audit trail and removes any doubt or confusion as to the exact amount of cash transferred. The lack of a receipt provides the opportunity for a dishonest employee to misappropriate funds and shift blame to other employees.

Recommendation: We recommend when currency is transferred between employees, a dated receipt should be generated and signed or initialed by both employees involved in the transaction.

Vault Cash

Vault cash is accessible to more than one individual. Whenever a currency supply is accessible to more than one person, it becomes vulnerable to theft or mysterious disappearance.

Recommendation: We recommend the vault cash be retained in a locked container under the exclusive control of one individual. If this is not practical, due to vacations, absences, breaks, etc., a second fund could be established which should also be retained in a lockable container under the exclusive control of one individual.

Common Cash Drawer

Several members of your staff work from a common cash supply. Whenever a supply of currency is accessible to more than one employee, it is vulnerable to theft or mysterious disappearance.

Recommendation: We recommend employees charged with the responsibility of handling currency be provided a lockable container under their exclusive control. This procedure will provide a valuable control, isolate balancing problems, and help minimize the probability of personnel problems in the event of a shortage.

Travelers Checks

All tellers have access to the supply of travelers checks. There is no individual accountability over these items. This makes them vulnerable to theft or mysterious disappearance.

Recommendation: We recommend placing the travelers checks in a locked container under the exclusive control of one employee. That person should conduct all sales or issue them to the tellers, via signed receipt, at the time of sale.

An alternative is to issue each teller a small supply of travelers checks. The tellers should keep these supplies in their cash drawers and balance them daily. A central bulk supply would still be necessary for replenishing the tellers. This supply should be in a locked container under the exclusive control of one person.

Nonbusiness Hours Teller Fund Storage

During nonbusiness hours, the teller trays are stored in a
[Click here and enter container type]. This procedure subjects any employee with access to the [Click here and enter container type] to accusations of misappropriating funds in the event of a shortage.

Recommendation: We recommend when teller funds are stored, the currency should remain in the individually locked containers provided, and the keys to the containers should remain with the tellers.

Teller Cash Drawers

Teller cash drawers are not always locked when the tellers leave their stations. Although employees must be trusted in order to perform their duties, an unlocked, unattended cash drawer invites mysterious disappearance losses.

Recommendation: We recommend when tellers leave their stations, they should lock their cash drawers and take their keys with them.

Teller Drawer Keys

Tellers leave the keys to their teller drawers in the [Click here and enter container type] during nonbusiness hours. In the event of a loss, lack of proper key control subjects every individual who had access to the teller drawer keys to accusations of misappropriating funds.

Recommendation: We recommend tellers retain possession of their drawer keys at all times and take them home at the end of the day.

Spare Keys

With the use of lockable containers, there arises the need to control access to spare keys. In the event of a loss, lack of proper spare key control subjects every individual who had access to the spare keys to accusations of misappropriating funds. This ease of spare key retrieval could easily lead to mysterious disappearance of funds.

Recommendation: We recommend spare keys to each lockable container be placed in a sealed envelope with the signature of the employee responsible for that container written over the seal. For additional protection, a strip of cellophane tape should be placed over the signature. If the need arises to access a container in the absence of the employee, two individuals acting jointly should initial the envelope, retrieve the key, access the container, and jointly verify the contents.

Vault Cash Keys

The vault cash teller leaves the drawer keys in the desk during nonbusiness hours. This allows the keys to be accessed by at least one other individual who also has the combination to the money safe. This ease of key retrieval could lead to mysterious disappearance of funds.

Recommendation: We recommend the vault cash teller maintain the drawer keys at all times. Additionally, the spare keys should be placed in a sealed envelope with the signature written over the seal. For additional protection, a strip of cellophane tape should be placed over the signature. If the need arises to access the vault cash in the teller's absence, two individuals acting jointly should initial the envelope, retrieve the key, access the container, and jointly verify the contents.

Teller Transactions

Tellers occasionally cash their own share drafts through their own teller cash drawers. Sound internal controls dictate that employees should not be able to conduct any transactions on their own accounts.

Recommendation: We recommend all employee transactions be conducted through another teller.

Employee and Family Member Transactions

You do not have written policies or controls prohibiting employees from performing transactions on their own or family member accounts. This exposes the credit union to possible loss through manipulation of personal or family member accounts that may not be detected by other employees.

Recommendation: We recommend establishing written policies prohibiting employees from processing transactions on their own or family member accounts. This restriction should include accounts belonging to members residing within the same household as an employee, even if not related. If possible, your data processing system should be programmed to restrict an employee from processing such a transaction.

Surprise Cash Counts

Our conversations with tellers revealed surprise cash counts have not been performed on at least a quarterly basis. Surprise cash counts are an excellent internal control. They serve as a detection device for unreported cash shortages and as a deterrent to "borrowing" from teller funds.

Recommendation: We recommend management make an effort to ensure surprise cash counts will be performed on at least a quarterly basis. Supervisory committee personnel, outside auditors, or management personnel can perform these cash counts. All cash supplies, including the vault cash and travelers checks, should be counted.

Surprise Cash Counts

Our conversations with tellers revealed surprise cash counts are not performed on all cash items. This could allow discrepancies to go undetected.

Recommendation: We recommend management make an effort to ensure surprise cash counts will be performed on all cash items on at least a quarterly basis. Supervisory committee personnel, outside auditors, or management personnel can perform these cash counts.

Restrictive Endorsements

When your tellers accept a check from a member, it is not immediately stamped with the credit union's restrictive endorsement. Once the payee has endorsed a check, it becomes a negotiable item.

Recommendation: We recommend when checks are accepted by your tellers, they should be immediately stamped with the credit union's restrictive endorsement.

Supervisory Override Controls

Supervisory override controls have not been implemented for your computer system. When properly utilized, supervisory overrides can ensure critical transaction processing is performed only with the approval of senior personnel.

Recommendation: We recommend management implement supervisory override controls for the computer systems. Someone without override authority should review the supervisory override report on a daily basis.

Supervisory Override Reports

Your data processing system does not generate a report of all transactions performed using a supervisory override. The lack of a report of these transactions negates the purpose of requiring an override to process the transaction. This also enables anyone with supervisory override authority to process unauthorized transactions without being questioned.

Recommendation: We recommend you research the possibility of obtaining a report, on a daily basis, of all transactions performed using a supervisory override. Procedures should then be established which provide for a regular review of this report. This review should be supplemented by an additional periodic review by the supervisory committee or outside auditor.

Supervisory Overrides

Your data processing system generates a report of transactions performed using a supervisory override. The lack of a regular review of this report negates the purpose of supervisory overrides, and enables any employee with supervisory override authority to perform unauthorized transactions without question.

Recommendation: We recommend establishing procedures which provide for a regular review of the supervisory override report. This review should include a spot-check of source documents. Particular attention should be paid to transactions on accounts belonging to employees and their family members.

Review of Supervisory Override Report

An individual who has override capabilities is reviewing the supervisory override report. An independent review of these transactions is important to ensure proper processing procedures are adhered to.

Recommendation: We recommend someone without override authority review the supervisory override report.

Computer Controls: See EDP Analysis Recommendations

Written Expense and Reimbursement Policy

You do not have a written expense and reimbursement policy. The lack of a written expense policy could lead to misunderstandings in regards to what expenses are reimbursable.

Recommendation: We recommend you develop a written expense policy to include approval requirements, documentation requirements, and a travel expense policy. The next higher level of supervision should approve all incurred expenses.

Expense Approval

The individual who approves expense accounts also has general ledger posting authority. This could allow fictitious expenses to go undetected.

Recommendation: We recommend the individual who approves expense accounts be restricted from accessing the general ledger processing function.

Corporate Expense Approval

Corporate expenses are sometimes reviewed and approved by a subordinate to the person who incurred the expenses. This violates sound internal controls by placing individuals in a potentially compromising position.

Recommendation: We recommend all corporate expenses be reviewed and approved by the next higher level of supervision.

Suspense Account Activity Review

The suspense account is reviewed by the employee responsible for posting to the account. This could allow errors, intentional or unintentional, to go undetected by management.

Recommendation: We recommend the suspense account be reviewed by supervisory personnel not responsible for posting to the account.

Overdraft Suspense Account Review

The overdraft suspense account is reviewed by the employee responsible for posting to the account. This could allow the employee the opportunity to hold overdrafts for their account or other accounts for an extended period.

Recommendation: We recommend the overdraft suspense account be reviewed by supervisory personnel not responsible for posting to the account.

Dormant/Inactive Account Monitoring

We noted there was no method in place to monitor activity to dormant/inactive accounts. Dormant/inactive accounts are frequently used to perform unauthorized transactions.

Recommendation: We recommend you contact your data processor to determine if a report can be established to identify transactions to dormant/inactive accounts, or require a supervisory override on these accounts. A review of these accounts should be established and all transactions verified. Additional consideration should be given to having the supervisory committee perform verifications of withdrawals to dormant/inactive accounts.

OR[Click here and edit]

Recommendation: We recommend you review your [Click here and enter report name] report which reflects activity to dormant accounts. Additional consideration should be given to having the supervisory committee perform verifications of withdrawals to dormant accounts.

Check Signature Machine

The counter on the check signature machine is not reconciled on a daily basis to the official count of checks used during operations. Unauthorized use of official checks could go unnoticed and cause a loss to the credit union.

Recommendation: We recommend reconciling the check signature machine counter to the official count of checks used during operations. A log should be maintained of this reconciliation, with the employee responsible initialing the log.

Signature Machine Control

We noted the signature machine and plates are not secured during nonbusiness hours. This could allow unauthorized use of the machine to process a stolen check.

Recommendation: We recommend the signature machine be locked or the plates be removed and locked in the [Click here and enter container type] during nonbusiness hours.

Access to Official Checks

Official checks are left in the printer overnight. This creates the opportunity for anyone gaining access to the office during nonbusiness hours to misappropriate funds.

Recommendation: We recommend safeguarding the official checks during business and nonbusiness hours. During business hours, the working supply of checks should be reconciled to the signature machine. At the close of business, the checks should be stored in a lockable container. Someone should verify the unused checks remain intact and in sequence, prior to being locked up for the night.

Bank Reconciliation

The employee who has the authority to sign credit union checks also performs the bank reconciliation. By allowing one person to perform both of these duties, manipulation of the credit union's checking account could occur and go unnoticed by management and the supervisory committee.

Recommendation: We recommend the duties of signing credit union checks and preparing the bank reconciliation be segregated. Although the practicality of this segregation of duties may seem somewhat limited, this procedure will assist in reducing losses.

Checking Account Reconcilement

The statements for the credit union's checking accounts have not been reconciled since [Click here and enter date]. The lack of completed reconcilements can result in differences and/or losses. Unauthorized activity can be concealed in this manner.

Recommendation: We recommend performing monthly reconcilements of all credit union checking accounts. Any unresolved differences should be brought to management's attention immediately. Differences not resolved within 90 days should require the attention of senior management for appropriate action.

Mail Deposits

Deposits received in the mail are opened and verified on a daily basis by one employee. In the event of a discrepancy in a deposit, or if an empty envelope was mailed, this employee would be placed in an unfair position.

Recommendation: We recommend the mail be accessed and the contents be verified by two employees acting jointly.

Night Depository

The contents of your night depository are opened and verified on a daily basis by one employee. In the event of a discrepancy in a deposit, or if an empty envelope was deposited, this employee would be placed in an unfair position.

Recommendation: We recommend the night depository be accessed and the contents be verified by two employees acting jointly. They should post the contents in a log and both sign the log entry.

Night Depository

The contents of your night depository are opened and verified on a daily basis under dual control. However, the dual control features of the container are not being utilized.

Recommendation: We recommend assigning the key and combination for the container to different employees. It will then require two people acting jointly to access the container's contents.

Night Depository

Proper procedures are used for opening and inventorying the contents of the night depository (dual custody). However, no log is kept of that inventory. If a member claims a deposit is missing, the lack of any written documentation to the contrary may make it difficult to resolve in favor of the credit union.

Recommendation: We recommend keeping a daily log of the contents of the night depository. Both employees conducting the inventory should sign the log entry.

Overdrawn Account Policy

There is no written policy regarding the processing of overdrawn share/share draft accounts. Lack of a written policy can lead to confusion regarding procedures, which in turn can lead to misunderstandings and violations of intended policies.

Recommendation: We recommend a formal board approved policy be formulated regarding the processing of overdrawn accounts.

Share Draft Policy

There is no written policy regarding share draft accounts. Abuse of share draft accounts through errors, misinterpretation of policy, and employee dishonesty is a major concern. Some sources of loss from share draft programs include nonassessment of fees, overdrawn accounts, and kiting.

Recommendation: We recommend you develop a share draft policy, have the policy approved by the board, and include this approval in the board minutes. Please refer to "Setting Share Draft/Checking Guidelines" (CRM-260) for items to include in this policy.

Funds Availability Policy

Regulation CC governs the availability of funds deposited. While credit unions must safeguard against bad checks, they also must protect the rights of members under Reg CC. Written procedures governing funds availability communicate an understanding of Reg CC, establish guidelines for placing holds on drafts, determine appropriate actions when holds are needed, and thereby protect the best interest of all involved.

Recommendation: We recommend you obtain a copy of Reg CC, develop a policy for your credit union, and communicate it to your membership.

Fraud Policy

We discussed the importance of a written fraud policy. The adoption of such a policy provides guidance for the credit union if embezzlement occurs. It also establishes a "tone from the top" that fraud by employees will not be tolerated. Please refer to "Development of a Credit Union Fraud Policy" (CRM-261) which is enclosed with this report.

Bondability Verification

As we discussed, the information necessary to verify the bondability of your existing employees will be submitted to Corporate P&C Underwriting for processing. Information to process new employees was also left with you.

No Recommendations:

We reviewed your internal control exposures. We have no recommendations in this area.

Forgery Control Analysis

Contract #: _____

	N/A	NoRec	Rec
1. Are signatures witnessed?			
2. Is positive identification required before witnessing signatures?			
3. Are signatures compared to dependable documents?			
4. Have employees been instructed in forgery detection techniques?			
5. Is the type of identification listed on the front of cashed checks?			
6. Is the reprinted identification on checks checked against positive identification?			
7. Are check holds used?			
8. Are employees trained: • to be on the lookout for fake identification? • to watch for signs of uneasiness? • in what to do if they recognize a forged document?			
Other Forgery Concerns:			

FCA

FORGERY CONTROL RECOMMENDATIONS TO EDIT IN GREAT BRITAIN

FCA1

Signature Witnessing

Employees do not always witness signatures on member documents. If the signature is contested, the courts will closely evaluate the witnessing process.

Recommendation: We recommend documents (checks, loans, etc.) be signed in front of employees, even if it means resigning documents.

FCA2

Positive Identification

[No standard recommendation]

FCA3

Signature Verification

When a member makes a request through the mail for an address change, the signature on the letter is not always compared to the membership card to determine authenticity. The lack of this procedure could allow an account to be diverted and used in a fraudulent manner.

Recommendation: We recommend signatures on all mail requests be compared to the membership card for authenticity. If doubt exists after making the comparison, direct telephone contact with the member should be made to confirm confidential information known only to the member.

FCA4

Forgery Detection Techniques

[No standard recommendation]

FCA5

Member Identification

In discussions with tellers, we learned the type of identification presented by your members is not always listed on the front of cashed checks. Requiring positive identification for member transactions will reduce the possibility of forgery.

Recommendation: We recommend when tellers request positive identification before cashing member checks, the type and identifiers of the identification should be listed on the front of the checks.

FCA6

Member Identification

[No standard recommendation]

FCA7

Check Holds

There are no holds placed on member check deposits. The funds are immediately available for withdrawal and increase the chance of losses from forgery.

Recommendation: We recommend you institute a check hold policy to reduce the probability of forgery losses. The adopted policy should conform to all federal and state regulations dealing with the availability of funds.

FCA8

Employee Training

Forgery schemes continue to multiply in recent years. Many credit unions have been seriously affected by various fraudulent schemes. These losses can be minimized through reasonable, yet effective, security measures.

Recommendation: We recommend training sessions be conducted with all employees to alert them of potential forgery techniques and their detection. The training should include signature forgery, comaker forgery, fake identification schemes, and potential manipulation or counterfeiting of cashier's checks/money orders. Credit union policy should dictate the use of a check hold system to protect against potential fraudulent member deposits. Please refer to "Managing Risks of Member Forgery and Fraud" (CRM-146) which is enclosed with this report.

Standard

Forgery Control Procedures

We found several prudent procedures being used to minimize the probability of loss due to forgery. Since forgery represents a major source of loss, we recommend a periodic review by management on such procedures. Please refer to "Managing Risks of Member Forgery and Fraud" (CRM-146) which is enclosed with this report.

FCA NO Recommendations

We reviewed your forgery control exposures. We have no recommendations in this area.

Fraudulent Deposit/Forgery Analysis

Contract #: _____

I. New Accounts	NoRec	Rec
A. Are new accounts flagged on the system for at least 90 days?		
B. Does the credit union utilize extended hold exceptions available under Reg CC for new accounts? **Note**: A problem may exist if holds are placed on deposits that exceed a monetary threshold. Dishonest members may make several deposits for amounts just under the threshold thereby avoiding check holds. To address this risk, consideration should be given to placing holds on aggregate deposits made on a single day.		
C. Are new members' identity verified and is the ID photocopied and retained (the driver's license should be photocopied for check cashing identification purposes)? • Are two pieces of identification required? **Note**: Some states may prohibit photocopying driver's licenses. The specialist should verify this in the state they are working.		
D. Is there a waiting period before a member can obtain ATM cards, debit cards, credit cards, audio response access, or home banking access? At a minimum, does the credit union have a reduced daily withdrawal limit for new ATM/debit cardholders and a reduced daily purchase limit for debit cards until a relationship is established?		
E. Do new account procedures exist in writing? • Do the written procedures adequately address procedures for opening accounts in-person/fax/mail/Internet? • Do the written procedures adequately address the method of verifying the applicant's eligibility? • Do the written procedures address the use of an early warning system (i.e., an AVS) or verification service (i.e., ChexSystems)? • Do the written procedures address underwriting procedures in approving checking account, debit, and/or ATM cards? • Do the written procedures address the use of account codes or flags to indicate new account status? • Are the procedures effectively communicated to employees during periodic staff meetings?		
F. Are employees trained in new account fraud?		
G. Are new members verified with reputable sources (Employer, Telecheck, Credit Report, ChexSystems, and address verification services)?		
H. Is ChexSystems used to screen all new members or just new or existing members requesting checking accounts?		
I. Is the membership application initialed by an employee to indicate proof that a ChexSystems report was run for the applicants? • Are joint account owners run through ChexSystems?		
J. Are new members granted a checking account, ATM/debit card, or audio response/home banking access if they have a ChexSystems record? Note**: New members with a ChexSystems record should only be allowed to have a savings account.**		
K. Are the accounts of members with a ChexSystems record coded or flagged on the system for at least 12 months to signify "high risk" account status?		
L. Are extended holds (i.e., no less than 9 business days) placed on deposits made to "high risk" accounts?		

II. Fraudulent Deposits	NoRec	Rec
A. Does the credit union have a written check hold policy?		
B. Does the credit union have a written check cashing policy?		
C. Is the credit union's funds availability policy posted in a conspicuous location of the lobby and proprietary ATMs?		
D. Are employees trained on Federal Reserve Regulation CC?		
E. Are check holds used on over-the-counter deposits?		
F. Are automatic holds put on ATM deposits? **See note on page 4**. • Proprietary ATMs (Reg CC allows a 2 business day hold on proprietary ATM deposits) • Nonproprietary ATMs (Reg CC allows a 5 business day hold on nonproprietary ATM deposits)		
G. How often are ATMs balanced (i.e., deposits retrieved from the machine and verified)? **See note on page 4.**		
H. Are cash letters sent daily?		
I. Are operating systems (ATM, debit card, share draft, and ACH) integrated to reduce the risk of negative balances from occurring? • Does the DP system identify multiple branch transactions performed on the same day?		
J. Are checks from out-of-town credit unions or banks scrutinized?		
K. Does the credit union verify funds on large checks?		
L. Are members allowed to cash/deposit checks made payable to a business (if the member does not have a business account)?		
M. Are employees trained in identifying altered checks? • Do tellers look for erasure marks and blots/blurs? • Do employees look closely for alteration of payee? • Are the "amount" sections of instruments reviewed for alterations? • Do employees verify perforations on checks prior to accepting? • Is the printing on the check reviewed for consistency (ink, letter styling)? • Do tellers make certain the written amount matches the numeric?		
N. If the check is made out to two people, have both signed and provided ID?		
O. Are employees trained to compare the Fed District number in the routing number to the bank's address for reasonableness?		
P. Do employees look for the term "nonnegotiable" on the instrument?		
Q. Are tellers trained on common check security features?		
R. Do tellers verify sufficient collected funds in the account before cashing a member's check?		
S. Do employees look for the following indicators of a potential swindler? • Member gets angry when asked for information • Nervous or impatient with teller • Unusual address/temporary address • No phone number • Does not want to have a check verified • Tries to distract teller or pretends to know other employees to give impression they are known to them		
T. Are third party checks rejected/scrutinized?		
U. Do tellers verify that a check is not stale dated (over 6 months old) or postdated? **Note**: According to the UCC, a bank is under no obligation to pay a check that is more than 6 months old.		
V. Are teller audits completed to determine their adherence to check cashing/deposit availability guidelines?		

II. Fraudulent Deposits (continued)	NoRec	Rec
W. Are SCAM Alerts distributed to all applicable employees? **Note**: To be effective, a history of the SCAM Alerts should be maintained for the tellers to review on a periodic basis.		
X. Are extended hold exceptions used if kiting is suspected? **Note**: If kiting is suspected, the credit union should invoke the Reg CC exception, Reasonable Cause to Doubt Collectibility. This allows the credit union to extend holds of up to 5 additional business days for local checks (total of 7) and 6 additional business days for nonlocal checks (total of 11).		

III. Forgery		Rec
A. Do tellers witness members endorsing checks (whether it is for deposit, split deposit, or payment) and signing withdrawal slips at the counter after requesting ID?		
B. Do employees use a driver's license or state ID card plus a second piece of identification to verify a member's identity? **Note**: Some state ID cards are not reliable for verifying a person's identity because they can be obtained from sources other than the state. The specialist should investigate the reliability of state ID cards for the state in which they are working as well as the adjoining states.		
C. Do employees verify physical description (i.e., sex, height, weight, birth date) on ID with the appearance of the individual?		
D. Do employees use the photocopied (or imaged) driver's license to verify identity if available? **Note**: Some states may prohibit photocopying driver's licenses. The specialist should verify this in the state they are working.		
E. Are expiration dates on IDs checked?		
F. Is the type of identification and identification number along with the expiration date listed on the front of cashed checks and withdrawal slips? **Note**: Reg CC has certain endorsement standards for the back of checks. Recording the driver's license information on the back of checks may make the endorsement illegible.		
G. Is the preprinted information on checks compared to information listed on the identification?		
H. Are employees trained to spot fake identification?		
I. Are signatures compared to dependable documents if driver's license or state ID is not available?		
J. Have employees been trained on forgery detection techniques?		
K. Does the credit union verify sufficient collected funds before cashing on-us checks?		
L. Are on-us checks cleared immediately?		
M. Are nonmembers allowed to cash on-us checks in the drive-up?		
N. Does the credit union fingerprint nonmembers when cashing on-us checks?		
O. Are telephone numbers obtained and verified from nonmembers presenting on-us checks for payment?		
P. Is the drawer's signature verified if an on-us check is being cashed by a nonmember? At a minimum, the credit union should establish a monetary threshold for verifying signatures (i.e., any item exceeding $250).		
Q. Is there a monetary threshold in place for generating calls to members to verify they have written a check to a nonmember?		

IIII. Insurance Coverage	NoRec	Rec
A. Does the credit union have fraudulent deposit, forgery, and other alteration coverage?		

V. Shared Branches	NoRec	Rec
A. Has the credit union provided the shared branch coordinator with written instructions on the use of check holds?		
B. Has the credit union established procedures with the shared branch coordinator to report or fax checks exceeding a predetermined dollar amount?		
C. Does the credit union limit the amount and type of payroll checks the shared branches can cash?		

ATM Note:

A problem may exist if holds are placed on deposits that exceed a monetary threshold. Dishonest members may make several deposits for amounts just under the threshold thereby avoiding check holds. To address this risk, consideration should be given to placing holds on aggregate deposits made on a single day.

Another problem may arise for proprietary ATMs that are not serviced (i.e., deposits retrieved) on a regular basis. According to Reg. CC, the hold period starts to run on the banking day on which the funds are deposited**. Furthermore, Section 229.19 states: "Funds deposited at an ATM that is not on, or within 50 feet of, the premises of the depository bank are considered deposited** on the day the funds are removed from the ATM **if funds normally are removed from the ATM not more than two times each week." Section 229.18 c (2) requires a special notice to be posted to the off-premise ATM from which deposits are not removed not more than two times each week. The notice must disclose the days on which deposits made at the ATM will be considered received. The following example illustrates this point:**

- A credit union's off-premise ATM is scheduled for servicing on Mondays and Thursdays
- Funds deposited after Thursday's cut-off time up to Monday's cut-off time are considered to be received (deposited) on Monday (hence the two day hold starts to run on Monday)
- Funds deposited after Monday's cut-off time up to Thursday's cut-off time are considered to be received (deposited) on Thursday (hence the two day hold starts to run on Thursday)

The specialist should recommend servicing off-premise ATMs on a regular basis. If the credit union is not willing to implement regular servicing of the ATM, the specialist should determine if the credit union's data processing system can be set up to offer longer holds.

FRAUDULENT DEPOSIT/FORGERY RECOMMENDATIONS TO BE EDITED IN GREAT BRITAIN NEW ACCOUNT FLAGS

New accounts are not flagged or coded on the system. Without new account flags or codes, tellers may not notice it is a new account, and may fail to exercise extra caution.

Recommendation: You should flag or code new accounts on the system for at least 90 days.

New Account Holds

Extended holds are not placed on deposits made to new accounts (checking and savings). Failure to place extended holds on new accounts increases your exposure to fraudulent deposit losses.

Recommendation: Extended holds should always be placed on deposits made to new accounts. For new checking accounts, Reg CC allows extended holds during the first 30 days after the account is opened. Since Reg CC does not apply to savings accounts, you can choose any availability schedule for deposits made to these accounts.

New Member Identification

The driver's license of new members is not photocopied and retained with the membership card. This has become a popular loss prevention tool for credit unions as it assists in identification efforts.

Recommendation: We recommend obtaining a photocopy of the driver's license of new members. The copy should be attached to the membership card. Prior to implementing this, you should verify that state law permits photocopying of driver's licenses.

Waiting Periods

You do not have a waiting period before new members are eligible to receive ATM or debit cards. A favorite option for scam artists is to request ATM or debit cards when the account is first opened. This provides them with a vehicle to withdraw funds from their fraudulent deposits or to make fraudulent deposits through the ATM network for subsequent withdrawal.

Recommendation: A waiting period should be established (e.g., 30 to 60 days) before new members are eligible to receive ATM or debit cards. An alternative is to issue an ATM or debit card with a low daily withdrawal limit (e.g., $50).

Written Procedures

You do not have written procedures to follow when opening new accounts. The lack of written procedures may create misunderstandings and increases your exposure to new account fraud.

Recommendation: We recommend you develop written procedures for the new account process. At a minimum, the procedures should include the following:

- The method of verifying eligibility if the membership applicant is employed by a select employee group.
- The method of verifying family membership eligibility.
- The use of an address verification service and/or ChexSystems as tools in screening new members.
- The requirement to code or flag new accounts on the system.
- The use of extended check holds on deposits made to new accounts.

New Account Fraud Training

Employees do not receive training on new account fraud. Failure to train employees on new account fraud increases your exposure to fraudulent deposit losses.

Recommendation: Employees should receive training on new account fraud. The training should address new account fraud scenarios and new account screening tools to include extended check holds.

Verification Services

You are not using a verification service to screen new accounts. Verification services have become increasingly important as fraudulent deposit losses associated with new account scams are increasing at an alarming rate. Sources such as credit reports, address verification services, and ChexSystems are valuable tools to use in screening new accounts.

Recommendation: We recommend you use a verification service in your efforts to reduce fraudulent deposit losses associated with new account scams.

Verification Services

You are not using a verification service to screen new accounts. Verification services have become increasingly important as fraudulent deposit losses associated with new account scams are increasing at an alarming rate. ChexSystems is a valuable tool in screening new accounts.

Recommendation: We recommend you use ChexSystems to screen new accounts. Individuals with a record at ChexSystems should **not** be allowed to have a share draft account, ATM/debit card, and audio response/home banking access.

In addition, you should consider using an address verification service, which helps identify potential fraud by comparing addresses and phone numbers to ensure the zip codes and prefixes are compatible. They also compare the address to known mail drops, prisons, hospitals, and previous fraud addresses.

Membership Application

Employees do not initial or sign the membership application to indicate a ChexSystems inquiry was made. New accounts may be opened without validating the individuals through ChexSystems.

Recommendation: We recommend employees sign or initial the membership application to indicate a ChexSystems inquiry was performed.

ChexSystems Records

You are using ChexSystems as a screening tool in your new account process. However, new members with a ChexSystems record are allowed to have a checking account and ATM card. This practice increases your exposure to fraudulent deposit losses associated with new account scams.

Recommendation: Individuals with a record at ChexSystems should **not** be allowed to have a share draft account, ATM/debit card, and audio response/home banking access.

System Support

Accounts belonging to members with a ChexSystems record are not coded or flagged on the system to signify "high risk" account status. Tellers may unknowingly process transactions on accounts considered to be high risk without exercising extra caution. This increases your exposure to fraudulent deposit losses associated with new account scams.

Recommendation: You should code or flag accounts belonging to members with a ChexSystems record to alert all frontline staff that extra caution should be exercised. The code or flag should remain on the account for at least 12 months. After 12 months, a new ChexSystems inquiry should be made to determine if problems may have surfaced that were reported by other financial institutions.

Check Hold Policy

The written check hold policy is incomplete. Incomplete policies can result in inconsistencies by employees.

Recommendation: We recommend you expand your written check hold policy to include holds on deposits made to "high risk" accounts (i.e., accounts belonging to members with a ChexSystems record). Check holds of **no less than 9 business days** should be used on deposits made to these accounts.

Check Hold Policy

You do not have a written check hold policy. Lack of written policies can lead to misunderstandings.

Recommendation: We recommend you develop a written check hold policy. The following points should be considered:

- Age of account (new account versus established account). A significant number of fraudulent deposit schemes are perpetrated on newer accounts (less than one year old). Extended holds should always be placed on deposits made to new accounts. Regulation CC allows you to choose any availability schedule for deposits to new checking accounts (accounts less than 30 days old), with the exception of certain next-day items.

You can choose any availability schedule for deposits made to savings accounts, as Reg CC does not apply to them. Tellers should exercise extra caution on the minimum balance share accounts that are less than one year old. Holds of no less than 7 business days should be placed on deposits made to these accounts. Furthermore, check cashing for these accounts should be limited to known company payroll checks only.

- The check hold policy should address items subject to next-day availability as defined in Reg CC. More importantly, the guidelines should address hold periods on local and nonlocal checks that are not subject to next-day availability. Reg CC allows a 2 business day hold on local checks and a 5 business day hold on nonlocal checks.
- Reg CC exception holds should be clearly stated in the policy. Reg CC allows an exception to the 2 or 5 day availability schedules for deposits made to share draft accounts for the following situations:
  - New accounts (less than 30 days old)
  - Large deposits (over $5,000)
  - Returned items
  - Repeated overdrafts
  - Reasonable cause to doubt collectibility
  - Emergency conditions

Check Cashing Policy

You do not have a written check cashing policy for your teller operations. Lack of a check cashing policy could cause losses to your credit union.

Recommendation: We recommend you develop a written check cashing policy. At a minimum, the policy should address the following:

- Identification requirements for cashing checks for members and nonmembers.
- Maximum amount of checks the credit union is willing to cash for members and nonmembers.
- Maximum amount of cash back on split deposits.
- Requirements for holding sufficient collected funds in the account of a member presenting a check for payment drawn on another institution.
- Requirement for verifying sufficient collected funds in an account before cashing an on-us check and to clear the item immediately.

Funds Availability Policy

Your funds availability policy is not posted in a conspicuous location of your lobby. This may place you in violation with Reg CC.

Recommendation: We recommend posting your funds availability policy in a conspicuous location of your lobby and at proprietary ATMs as required by Reg CC.

Regulation CC

Employees are not trained on Federal Reserve Regulation CC (Reg CC), which may place you in violation with the regulation. According to Reg CC, financial institutions are required to establish procedures to ensure compliance with the regulation and to provide a copy of these procedures to all employees who perform duties affected by the regulation. Employees who are not adequately trained may not know when to place holds on deposits (including extended holds) and how to notify members that funds are being held.

Recommendation: We recommend you provide Reg CC training to those employees who perform duties affected by the regulation. Your Federal Reserve District office should be able to assist you in your training efforts.

Check Holds

Check holds are not placed on member deposits to checking and/or savings accounts. The lack of check holds on member deposits increases your exposure to fraudulent deposit losses.

Recommendation: You should use check holds on member deposits. Check holds on deposits made to share draft accounts are governed by Reg CC. Since Reg CC does not cover savings accounts, you can choose any availability schedule for deposits made to these accounts.

ATM Deposits

Members receive immediate credit on deposits made through the ATM network. This practice increases your exposure to fraudulent deposit losses.

Recommendation: You should use check holds on deposits made through the ATM network. Reg CC allows holds up to 2 business days on deposits made at proprietary ATMs and 5 business days on deposits made at nonproprietary ATMs.

ATM Balancing

Your ATMs are not balanced (i.e., deposits retrieved) on a daily basis. A member may deposit a fraudulent check (or an empty envelope) in your ATMs that would not be discovered until the ATMs are balanced. Any check hold placed on the deposit may expire before the items are verified. This practice increases your exposure to fraudulent deposit losses.

Recommendation: We recommend balancing the ATMs on a daily basis. The cash letter containing the ATM deposits should be sent for collection daily at a minimum.

Cash Letter

Cash letters are not sent daily, which delays the check clearing process. This creates a delay in receiving notice from the institutions on which checks are drawn that items are being returned unpaid to your credit union. This practice increases your exposure to fraudulent deposit losses.

Recommendation: At a minimum, cash letters should be sent for collection daily.

Operating Systems

[No standard recommendation]

Nonlocal Checks

[No standard recommendation]

Large Items

Tellers do not call to verify funds on large checks presented. Tellers may unknowingly accept checks that may not clear.

Recommendation: We recommend implementing a procedure for tellers to call to verify funds on large items presented (e.g., checks more than $1,000).

Checks Payable to Businesses

Members are allowed to cash or deposit checks made payable to a business even though the member is not the payee listed on the check. This practice increases your exposure to forgery losses.

Recommendation: Tellers should never accept checks from members who are not listed as being the payee, including checks made payable to businesses.

Check Alterations

Employees are not adequately trained to identify checks that have been altered. This training is vital in order to reduce your exposure to forgery losses.

Recommendation: Tellers should be trained to examine items for the following characteristics of altered checks:

- Erasure marks on the checks.
- Alteration of the amount, both numbers and words.
- Numbers in the amount sections of the check that look “unnaturally” close together.
- Written amount agrees with the numbers.
- Perforations on checks.
- Irregular or inconsistent printing on the check.
- Improbable combination of payees, such as ABC Company or John Smith.
- “Cloudy” or “bleached” areas on the check.
- Ballpoint impressions on the check that contain no ink.
- Different handwriting styles on the check as well as different colors of ink.

Joint Payees

When tellers receive checks payable to two or more people, they do not require the signature of all payees nor do they properly identify them. This increases your exposure to forgery losses.

Recommendation: Tellers should always require the endorsement of all payees unless the check is deposited to an account held by all payees.

Federal Reserve Districts

Counterfeit checks present an exposure to credit unions. Changing the Federal Reserve District routing and transit number causes checks to be routed incorrectly. Your tellers have not been trained on this technique, which increases your exposure to fraudulent deposit losses.

Recommendation: We recommend you provide training to tellers on this common characteristic of counterfeit checks. Tellers should compare the Federal Reserve District number (i.e., the first two digits in the routing and transit number) to the location of the institution on which the check is drawn for reasonableness.

Nonnegotiable Checks

Tellers do not examine checks for the term “nonnegotiable”. Careless examination of checks by tellers increases your exposure to loss of accepting nonnegotiable instruments.

Recommendation: We recommend tellers carefully examine checks presented for deposit or payment for evidence of nonnegotiability.

Check Security Features

Tellers have not received training on common check security features. This training is extremely important for tellers to properly authenticate checks presented. The lack of training in this area increases your exposure to fraudulent deposit losses.

Recommendation: We recommend you provide training for tellers on the common check security features. This includes, but is not limited to, security screens, watermarks, microprinting, chemical voids, and void pantographs.

Verifying Collected Funds

Tellers do not verify the existence of sufficient collected funds in the accounts of members presenting checks for payment. This increases your exposure to fraudulent deposit losses in the event a deposited check is returned unpaid.

Recommendation: Tellers should always verify sufficient collected funds in members’ accounts before cashing checks presented. A hold should be placed on the account up to the amount of the cashed check if sufficient collected funds exist. The length of the hold placed on the funds should be 2 or 5 business days depending on whether the item is local or nonlocal. The hold period should be increased if any of the Reg CC exceptions apply. If sufficient collected funds do not exist, the member should be required to deposit the check with the appropriate holds being placed.

Scam Artist Behavior

Various forgery and deposit scams have increased over the years causing large losses for credit unions. Criminals perpetrating these scams tend to behave differently than typical members. Employee training is critical in identifying a potential scam.

Recommendation: We recommend providing training for employees on common scams and behavior exhibited by scam artists. Common scams committed by criminals include identity theft, new account scams, and split deposit scams. Characteristics of a scam artist's behavior include:

- Nervousness
- Overly complimentary or talkative
- Distracting
- Rudeness

Third Party Checks

Tellers accept third party checks without verifying the identity of the original maker of the item. Third party checks present an increased risk, as it is very difficult to verify the intent of the original maker who endorsed the item over to the individual who presented it. Accepting third party checks increases your exposure to forgery losses.

Recommendation: We recommend extreme caution be exercised when cashing third party checks. Telephone verification to the check originator and payee may be necessary for large items.

Stale/Postdated Checks

Tellers do not examine checks presented to verify the items are not stale (over six months old) or postdated (future dated checks). This increases your exposure to loss from items that may not be properly payable.

Recommendation: Tellers should always carefully examine checks presented for stale and postdated items. Furthermore, stale and postdated items should not be accepted. This is based on the following:

- Stale dated checks: according to the U.C.C. (Section 4-404), *A bank is under no obligation to a customer having a checking account to pay a check, other than a certified check, which is presented more than six months after its date, but it may charge its customer's account for a payment made thereafter in good faith*. The safest course of action is to refuse the check since the credit union has no knowledge that the institution will pay the item in good faith.
- Postdated checks: according to the U.C.C. (Section 4-401), *A bank may charge against the account of a customer a check that is otherwise properly payable from the account, even though payment was made before the date of the check, unless the customer has given notice to the bank of the postdating describing the check with reasonable certainty*. Again, the safest course of action is to refuse the check since the credit union has no knowledge that the maker has given notice to the institution of the postdating.

Teller Audits

Teller audits are not performed to verify compliance with your check hold/cashing policies. The lack of periodic audits increases your exposure to fraudulent deposit and/or forgery losses due to noncompliance with your existing policies.

Recommendation: We recommend performing periodic audits (e.g., monthly) to verify tellers are complying with your check hold and check cashing policies.

SCAM Alerts

SCAM Alerts are not shared and discussed with the appropriate employees. SCAM Alerts are intended to notify credit unions of scams occurring in the area. Employees would have no knowledge of these scams since the SCAM Alerts are not shared and discussed with them.

Recommendation: We recommend sharing and discussing SCAM Alerts with the appropriate employees. Furthermore, the SCAM Alerts should be maintained in a file or log so employees can review them on a periodic basis.

Check Kiting

Tellers do not place extended holds on deposits made by members who are suspected of check kiting. The lack of extended holds placed on deposits made by members suspected of check kiting increases your exposure to fraudulent deposit losses.

Recommendation: We recommend tellers place extended holds on deposits made by members who are suspected of check kiting. Reg CC allows an exception to the 2 or 5 day availability schedule for local and nonlocal checks if an institution suspects an account holder is involved in a check kiting scheme. This falls under the exception for *Reasonable Cause to Doubt Collectibility* and it allows you to place a hold of up to 7 business days for local checks, and 11 business days for nonlocal checks. The extended hold must be disclosed to the member in writing (e.g., the credit union has received confidential information that the check may not be paid).

Signature Witnessing

Tellers do not always witness members endorsing the back of checks or signing withdrawal slips. This practice increases your exposure to forgery losses.

Recommendation: Tellers should always witness members endorsing the back of checks or signing withdrawal slips. If members present preendorsed checks or withdrawal slips, tellers should request the member to sign again so the signature can be witnessed. This procedure should be utilized for both lobby and drive-up transactions.

Identification Procedures

Tellers do not always request a member’s driver’s license to verify their identity. This practice increases your exposure to forgery losses.

Recommendation: Tellers should always request a driver's license to verify the identity of members who are not recognized by both face and name. The driver's license number along with the expiration date should be recorded on the face of checks presented and on withdrawal slips.

Physical Descriptions

Tellers request and examine a member's driver's license to verify their identity. However, they do not compare the physical description (sex, height, weight, and birth date) listed on the driver's license with the appearance of the member.

Recommendation: Tellers should always compare the physical description listed on the license with the appearance of the member. If there are any discrepancies, a second piece of identification should be required or the signature should be verified.

Photocopied Identification

Tellers do not use the photocopied driver's license to verify a member's identity when the member has no form of positive identification with them. The purpose of obtaining a photocopy of the driver's license when the account is opened is to assist in identification efforts. This increases your exposure to forgery losses.

Recommendation: Tellers should always use the photocopied driver's license to verify a member's identity when the member has no form of positive identification with them.

Expiration Dates

Tellers do not check the expiration date on a member's driver's license when verifying their identity. An expired driver's license is not considered a valid form of identification.

Recommendation: Tellers should always check the expiration date on members' driver's licenses. The driver's license number along with the expiration date should be recorded on the face of checks presented and on withdrawal slips.

Identification Procedures

Tellers request and examine the driver's licenses from members they do not recognize. However, the driver's license number and expiration date are not recorded on the face of checks presented or on withdrawal slips. This information will assist the local law enforcement agency in their efforts to locate the individual if the item or withdrawal turns out to be fraudulent.

Recommendation: Tellers should always record the driver's license number and expiration date on the face of checks presented and on withdrawal slips.

Preprinted Information

The preprinted information listed on personal checks (i.e., name and address) presented by members is not compared to the information contained on the driver's license. This increases your exposure to forgery losses.

Recommendation: Tellers should always compare the preprinted information listed on personal checks presented by members with the information contained on the driver's license. If there are any discrepancies (e.g., the addresses do not match), a second piece of identification should be required.

Authenticity of Identification

Employees have not been trained on identifying fraudulent driver's licenses and state ID cards. Scam artists often use fraudulent identification when attempting to pass forged or fraudulent checks.

Recommendation: We recommend providing training for employees on identifying fraudulent driver's licenses and state ID cards. You should contact the secretary of state in your state as well as adjoining states for training material to use in assessing the authenticity of driver's licenses and state ID cards.

Signature Verification

Tellers do not verify a member's signature against the membership card when positive identification is not available. This increases your exposure to forgery losses.

Recommendation: Tellers should always verify a member's signature against the membership card when positive identification is not available. Requesting personal identifying information (e.g., account number, social security number, birth date, and mother's maiden name) is not a reliable method of verifying an individual's identity as it is easily obtained from other sources.

Employee Training

Many credit unions have been affected by various fraudulent schemes. These losses can be minimized through training.

Recommendation: We recommend providing training for employees to alert them of forgery techniques and detection. The training should include signature forgery and fake identification schemes. The training should also cover fraudulent checks (counterfeit checks and altered checks), check kiting, and split deposit schemes.

On-us Checks – Verification of Funds

Tellers do not verify sufficient collected funds before cashing on-us checks. This practice may result in negative balances from cashing on-us checks against accounts with insufficient collected funds.

Recommendation: Tellers should always verify sufficient collected funds in member accounts before cashing on-us checks.

On-us Checks – Clearing

On-us checks are not cleared immediately. Instead, these checks are included in the daily cash letter. If funds in the account are depleted before the draft is posted, you may be forced to reject a draft for which credit has already been granted.

Recommendation: Tellers should immediately clear on-us checks presented for payment. The items should be filed in a central location or with the tellers' daily work.

Nonmember Transactions in Drive-up

Nonmembers are allowed to cash on-us checks in the drive-up. Criminals prefer to use the drive-up facility because identity is difficult to establish. This increases your exposure to forgery losses.

Recommendation: All nonmembers should be required to come into the lobby where they can be properly identified before cashing their checks.

Fingerprinting Nonmembers

Many credit unions have introduced fingerprinting in their operations as a tool against forgery and check fraud. They have experienced a significant decline in forgery losses.

Recommendation: We recommend you consider fingerprinting in your operations. CUNA Mutual Business Services (800-356-5012) offers ID Print which is an inkless fingerprinting pad specifically designed to deter forgery and check fraud. The check presenter is asked to leave their thumbprint on the face of the check, between the memo and signature lines. Credit unions will not normally retain the fingerprint in their files but will share them with law enforcement officials to investigate check fraud. Credit unions should obtain a thumbprint in the following circumstances:

- A nonmember presents for cash payment either a member's check drawn on the credit union, or a credit union's cashier's or teller's check.
- A nonmember seeks to exchange a member's check for the credit union's cashier's check, teller's check, or money order.

Many credit unions also require all new members to provide their thumbprint on the membership card and all checks presented. In the event the new member issues a substantial number of overdrafts or deposits fraudulent checks, the credit union can provide the thumbprint to law enforcement officials. Credit unions can discontinue this practice after the account has become established.

Nonmember Information

Telephone numbers are not obtained and verified from nonmembers presenting on-us checks for payment. This procedure is intended to provide additional verification on nonmembers. The lack of such a procedure increases your exposure to forgery losses.

Recommendation: We recommend obtaining and verifying the telephone numbers of nonmembers who present on-us checks for payment. This procedure should be performed prior to cashing the on-us check. You may want to implement a monetary threshold (e.g., $250) before this procedure is required.

On-us Checks – Signature Verification

Tellers do not verify the maker's signature against the membership card when cashing on-us checks for nonmembers. This increases your exposure to forgery losses.

Recommendation: Tellers should verify the maker's signature against the membership card before cashing on-us checks for nonmembers. If you cash a high volume of low dollar on-us checks for nonmembers, you should consider establishing a monetary threshold (e.g., $100) for verifying signatures.

On-us Checks – Member Verification

Large dollar on-us checks presented for payment by nonmembers are not verified with the maker. This increases your exposure to large forgery losses.

Recommendation: Large dollar on-us checks presented for payment should be verified with the maker before cashing the items for nonmembers.

Forgery and Fraudulent Deposits

Your existing limit for Forgery and Fraudulent Deposit Coverage is $[Click here and enter amount]. Credit unions with a share draft program have been sued in forgery cases for damages as much as $1,000,000 due to disputes with banks concerning collection items. Any size credit union that offers share drafts has an exposure to catastrophic kiting losses. Credit unions have had $1,000,000 kiting losses.

Recommendation: We recommend you analyze and discuss with your account relationship manager this potentially catastrophic loss exposure.

Check Holds

Check holds are not placed on deposits made at shared branches. The existence of shared branches has made forgery and check fraud much easier to commit. Shared branch employees are less familiar with your members and have limited access to their account information. This increases your exposure to fraudulent deposit losses.

Recommendation: We recommend providing written instructions to your shared branch coordinator for imposing holds on your members' deposits.

Large Checks

There are no established procedures for shared branches to report large items presented by your members. Shared branch employees are less familiar with your members and have limited access to their account information. This increases your exposure to forgery and fraudulent deposit losses.

Recommendation: We recommend establishing a reporting requirement with the shared branch coordinator for large checks presented. The shared branches should fax large checks to your office for immediate investigation.

Payroll Checks

The credit union does not limit the type and amount of payroll checks that can be negotiated at a shared branch. Shared branch employees are less familiar with your members and have limited access to their account information. This increases your exposure to fraudulent deposit losses.

Recommendation: We recommend establishing instructions for the shared branch coordinator to limit the amount and type of payroll checks that can be negotiated at shared branches.

No Recommendations:

We reviewed your fraudulent deposit/forgery exposures. We have no recommendations in this area.

FIDELITY ANALYSIS

Contract #:	**Date:**
Address:	**Specialist:**
	Approved:

AUDIT CATEGORY	NC	OK	RPT	MF	CM
Employee & Family Member Accounts Overdrafts Share Draft Exceptions Journal Voucher Transfers Lending Exceptions (including credit cards) Dates Reviewed:_____					
Director/Officers/Appointees & Family Member Accounts Overdrafts Share Draft Exceptions Lending Exceptions Other Dates Reviewed: _____					
Fictitious / Unauthorized Loans					
Expenses Dates Reviewed:_____					
Deposits In Transit / Reconcilement Items Dates Reviewed:_____					
Canceled Checks Dates Reviewed:_____					
Share Withdrawals					
LP / LS Insurance Proceeds					
G/L Suspense Accounts Dates Reviewed:_____					
CDI / CLI Payments					
Closed Accounts					
Dormant Accounts					
Repossessed Collateral Dates Reviewed:_____					
Travelers Checks Dates Reviewed:_____					
Money Orders Dates Reviewed:_____					
Other:_____ _____ _____					

241-CRM-243 (R12/96)

Please comment below on any details, recommendations, or other notable findings you feel necessary to explain the situation itemized as exceptions. If Home Office personnel were contacted and/or directions were given, please note.

Who did you speak to in the Home Office? Detail your discussion and subsequent decisions made:

Please Note:

The Fidelity Analysis relies on your knowledge of Supervisory Committee' duties and responsibilities. The analysis is not designed as much for the RMS to redo or duplicate the Supervisory Committee's function, as it is for the RMS to interview and spot check what's being done so as to confirm it's done correctly. For example, evaluate how the Member Account Verification was done to determine whether or not it was done under the control of the SC to include everything from running tapes to stuffing and mailing envelopes and controlling those not delivered. Another example is, does the credit union effectively enforce the rotation and separation of duties.

The Risk Management Specialist should conduct **"Supplementary Audits,"** checking loan files for fictitious and unauthorized loans, checking the bank reconciliation for deposits in transit, checking suspense accounts to make sure they're cleared monthly, reviewing expense folders to confirm expenses are within reason and properly approved, and in general, come to a conclusion the credit union management is enforcing all internal and audit controls that are needed to discourage or detect internal dishonesty.

Refer to some of the questions in the bond application for other supplementary auditing suggestions.

ATM Analysis

Contract #: _____

IV. Physical Security

ATM Blanket Liability Endorsement	N/A	NoRec	Rec
A. Is the credit union storing more than the limit of their blanket ATM coverage?			

TL-15 Rated ATMs with > $100,000	N/A	NoRec	Rec
B. Are the ATMs properly alarmed?			

Location	Manufacturer Name & Model	Alarm Components	Total Currency

TRTL-15x6 Rated ATMs with > $300,000	N/A	NoRec	Rec
C. Are the ATMs properly alarmed?			

Location	Manufacturer Name & Model	Alarm Components	Total Currency

Business Hour ATMs	N/A	NoRec	Rec
D. Are the ATMs used/accessible 24 hours a day?			

Location	Manufacturer Name & Model	Alarm Components	Total Currency

Replenishment & Repair	N/A	NoRec	Rec
E. Are ATMs replenished Via Contracted Service? Maximum Transported: Insured Limit:			
F. Are ATMs replenished Via CU Employee? Maximum Transported: Date:			
G. If CU employees repair or replenish ATMs during business hours are there written procedures?			
H. Are security measures in place to protect these employees?			

II. Internal Controls	N/A	NoRec	Rec
A. Preparation of ATM replenishments			
B. Verification of ATM receipts			
C. Holds used on ATM deposits			

D. Account Numbers printed on receipts			
E. Withdrawal/transfer limitations during live time or down time			
F. Lost/stolen card "hot card" updates			
G. Captured/returned ATM cards to include storage, dual control, and logs			
H. Card distribution (to members) controls to include encoding equipment/blank plastic controls and PIN/PAN number controls			

III. Member Safety	N/A	NoRec	Rec
A. Is there a written ATM security program? Does this include member education and standard safety procedures? Is CU aware of applicable state regulation compliance issues? Have there been any robberies which require follow-up action?			
B. Have you evaluated each ATM location to assure member safety? Good visibility, no concealment, lighting, mirrors, safe neighborhood, parking? Is 24 hour use appropriate? Is the area in and around the ATM, including the lighting, on a regular maintenance schedule?			
C. Is each ATM equipped with a camera? Does the ATM camera receive priority at night? Is film quality checked periodically?			

IV. Quick Cash Dispensers	N/A	NoRec	Rec
A. Are security measures in place for cash dispensers? Unauthorized access? Cameras? Shoulder Surfing? Truncated receipts? Pin distribution? Numerous transactions allowed? Withdrawal limitations? Replenishment procedures? Non-business hour currency cartridge storage?			
B. Do any machines (ATM or QCD) need to be anchored?			
C. Other ATM concerns:			

ATM ANALYSIS RECOMMENDATIONS TO BE EDITED IN GREAT BRITAIN

ATM Blanket Liability Endorsement

The ATM blanket coverage under your Corporate P&C bond limits coverage to $150,000 per ATM. In reviewing your ATM security, you have the necessary alarm system to store above this amount. We have informed Corporate P&C Underwriting of this and your ATM endorsement will be adjusted accordingly.

ATM Alarm Systems

The ATM blanket coverage under your Corporate P&C bond limits coverage to $150,000 per ATM. In reviewing the cash figures stored in the machine, we discovered you have exceeded this amount in your ATM.

Recommendation: If your currency requirements continue to exceed $150,000, you will need to add the following alarm components. We have contacted Corporate P&C Underwriting regarding this exception and your ATM endorsement will be adjusted accordingly.

- Audio Accumulator - which will detect noise resulting from hammering, drilling, etc.
- Heat Detector - which will detect heat resulting from a torch attack.
- Door Contact - which will detect unauthorized opening of the ATM door.
- Internal Line Security - the alarm system should be equipped with high-grade internal line security, which protects the alarm reporting line between the ATM alarm components and the alarm control panel. The specifications for this line security should equal or exceed Diebold's PLS II, Mosler's ILS, or LeFebure's FLS-1.
- External Line Security - the alarm system should be equipped with low-grade external line security, which protects the alarm reporting line between the ATM and the alarm reporting station. The specifications for this line security should equal or exceed Diebold's Multi-Guard II, Mosler's PAC-A, or LeFebure's PM 3101.
- External Line Security - the alarm system should be equipped with high-grade external line security, which protects the alarm reporting line between the ATM and the alarm reporting station. The specifications for this line security should equal or exceed Diebold's Multi-Guard V, Mosler's HLS, or LeFebure's LM 3101.

  An alternative is to use an Underwriters Laboratories Inc. (UL) rated "AA" radio frequency (RF) reporting system or a high-grade cellular system. The specifications for the cellular system can be found in "Cellular Alarm Installation Specifications" (CRM-336).
- Standby Power Supply - the alarm system should be equipped with a "fail-safe" standby reserve power supply which is capable of operating the alarm system for a minimum of 48 hours if electrical power is lost.
- Alarm Shunt - the alarm should be installed so that authorized persons will be able to enter the premises without disalarming the ATM.

ATM Alarm Systems

[No standard recommendation]

Business Hour ATMs

[No standard recommendation]

ATM Replenishment Service

As much as $[Click here and enter amount] has been transported by the service that replenishes your ATM. A review of their service contract indicated their limit of liability is $[Click here and enter amount]. The amount of cash transported by this service should be fully covered by their liability insurance. If the service is robbed while replenishing your ATM, you could sustain a loss.

Recommendation: We recommend you either negotiate your contract with the ATM replenishment service to increase their liability insurance, or reduce the amount of cash ordered for the ATM to comply with the liability limit in the contract.

Currency Transportation Guidelines

Employees are transporting up to $[Click here and enter amount] in cash for replenishment of the ATM. When transporting cash, a potential for loss exists. This can extend even beyond the amounts transported to include civil liability relating to employee and public safety.

Recommendation: We recommend using the following security guidelines as minimum standards for transporting cash:

- When transporting $50,000 or less, use one or more employees.
- When transporting between $50,000 and $100,000, use one employee and one armed guard.
- When transporting in excess of $100,000, use an armored car service.

ATM Security Program

Liability to ATM owners and operators is increasing because the public has become more conscious of security and safety expectations at ATMs. We did not see a security program which details employee safety when replenishing or repairing the machines.

Recommendation: We recommend developing and implementing methods of determining risk through an ATM program. A security program with written procedures to assure employee safety would be beneficial to everyone and provide for continuing evaluation and improvement of the program.

After Hours Security

Employees have responded to an alarm or out of service ATM at night. They enter these premises without a police escort. Such practice subjects your staff to serious risks if a perpetrator purposely set an alarm.

Recommendation: We recommend establishing written procedures for staff to follow in responding to alarms and ATM shutdowns. Under no circumstance should employees arrive to service an ATM at night without proper security.

ATM Replenishments

[No standard recommendation]

Verification of Deposits

One employee verifies the deposits from your ATM. When the credit union is in possession of a member's property in their absence, the property should be maintained under dual control at all times. If a less than honest member claimed a deposit was made when in actuality it was not, your employee could be placed in a compromising position, as it would be the member's word against that employee's.

Recommendation: We recommend two employees jointly verify ATM deposits.

Holds on ATM Deposits

You do not use holds on ATM deposits. These deposits can be withdrawn in their entirety over the teller counter or through the audio response system. If the deposits are returned uncollectible, you could suffer a loss.

Recommendation: We recommend you consider using holds on ATM deposits. You may wish to pursue the possibility of holding funds that exceed a monetary threshold such as $5,000.

Account Number Truncation

ATM receipts are currently printing the member's entire account number. People often leave their receipts at the ATM, or throw them in a trash receptacle nearby. Account numbers, particularly on debit cards, have been used to make counterfeit cards.

Recommendation: We recommend you have the account numbers truncated on the ATM receipts.

ATM Off-line Transfers

Your ATM system allows members to transfer between accounts when the system is in an off-line mode. There is no dollar limit to these transfers. The system will allow a share account to go negative to fund a share draft account. If these transfers are not discovered timely, the funds may be withdrawn from the share draft account. A negative position could occur.

Recommendation: We recommend the system not allow transfers in an off-line mode or restrict the transfers to a monetary limit.

Derogatory File Maintenance

The derogatory file which is used to identify lost, stolen, or abused cards is not being promptly updated. Lack of prompt updating of this file could result in losses to member accounts for which your credit union could be held liable.

Recommendation: We recommend the derogatory file for each ATM be updated on a prompt and consistent basis. Data on lost, stolen, or abused cards must be added to the file as quickly as possible.

Captured/Returned Cards

[No standard recommendation]

Card Distribution Controls

[No standard recommendation]

ATM Security Program

[No standard recommendation]

Member Safety

[No standard recommendation]

ATM Camera

Your camera surveillance system does not change during nonbusiness hours. There may be certain areas of the credit union that do not warrant continuous camera protection. Other more likely areas of concerns (ATMs, perimeter doors, etc.) should be prioritized during nonbusiness hours to assure an efficient surveillance system is in place.

Recommendation: You may consider switching more priority to the ATM camera, while still maintaining some camera coverage within the building.

Quick Cash Dispensers

[No standard recommendation]

ATM Security

Your ATMs have wheels installed on them. ATMs with wheels are an attractive burglary target.

Recommendation: We recommend these ATMs be secured by bolting them to the floor. Consideration should also be given to having the wheels removed.

Other ATM Issues

[No standard recommendation]

We reviewed your ATM exposures. We have no recommendations in this area.

Several commendable procedures and security measures were observed during the analysis. This report contains a review of physical conditions, practices, and procedures which represent increased elements of risk. The recommendations and/or requirements in this report are based upon statements made to us, as well as observed exposures and/or hazardous conditions. This report does not indicate that risks, not considered or observed, are adequately controlled.

COMMENTARY

This report may include recommendations and/or requirements. The definition for those terms is provided below:

A **recommendation** is our best advice of how to reduce loss, or the potential for loss, in a given area.

A **requirement** is a particular area of concern in which the credit union must comply with our solution, or negotiate an acceptable compromise for solution. Otherwise, underwriting action will be taken. The action could consist of lower coverage limits, higher deductibles, or a restrictive (exclusionary) endorsement.

In the written response you have agreed to submit, it is very important for the credit union to clearly indicate whether you will, or will not, adopt the individual recommendations and/or requirements.

SAMPLE RMA REPORTS

FOLLOWING ARE REPORTS THAT INCLUDE A FOLLOW UP ON A PAST RMA, AS WELL AS, AN ANALYSIS OF BRANCHES NOT ANALYSED DURING THE FIRST VISIT:

MAIN OFFICE AND ALL BRANCH LOCATIONS

FOLLOW UP ON REPORT DATED FEBRUARY 4, 2000

Some of the following is based on a review of recommendations made and management action taken after an on-site Risk Management Analysis was conducted at your main office (450 Cherry Street) on February 3, 2001. A copy of the original report was mailed to the credit union February 4, 2001.

BURGLARY ANALYSIS

Vault Alarm

A vault alarm system was recommended based on your Safe Deposit Box service and the potential liability exposures should member' property stored in the boxes be lost. Because liability risks associated with safe deposit box services have increased since 1999, this recommendation has been elevated to a "requirement" in US credit unions. Based on the growing desire to sue, I believe credit unions in Great Britain should also elevate safe deposit box vault alarm systems to a "requirement."

Requirement:

Review the vault-alarm recommendation and have it installed. Contact your CMG Risk Management Specialist if you have questions relative to the recommendation in the 1999 report. I'm sure they can help clarify any questions.

ROBBERY ANALYSIS

Armored Car Service

I compliment your staff's use and knowledge of armored car services at all offices. As recommended in the 2000 report, it's also important that they continue to monitor the amounts transported and the liability coverage provided by the armored car service.

Requirement: Credit union staff at each location should review your armored car coverage limits in relationship to what's transported. Ensure the limits in your armored car service contract cover the full amount of all your cash shipments. In the alternative, you should limit your cash shipments to the amount of liability provided.

Robbery Training

I noted during the analysis some robbery training has occurred but in most offices it has been over one year. Regular training to prepare all employees for a robbery is most important.

Recommendation: I recommend you consult with your CMG Risk Management Specialists. They can help you with your training needs. Set a goal to conduct such training at least every three months. Include all your guard services and local police in training. It is very important for all credit union staff, guards, and responding law enforcement to know what everyone is and will do before, during and after a robbery. Develop written procedures for your staff, the guards, and local law enforcement.

Post Robbery Trauma Training

Much can be done to assist robbery victims after a robbery.

Recommendation: As part of robbery training, include victim assistance training. For example encourage "non-judgmental" attitudes, victims to talk or vent. Help them deal with their guilt, fear, and sense of being out of control. Alert your Risk Management Specialist at CMG as soon as possible after a robbery.

Written Robbery Response Procedures

I compliment your use of armed and unarmed, uniformed and plain-cloths guards, and robbery alarm systems reporting to local police at each of your offices. Staff at each office indicated a general understanding of the guard's duties, practices, and procedures. Knowing exactly what guards and local law enforcement do and how they will respond to a robbery will help your staff feel more secure, more in control, and more prepared for robbery.

Requirement: In addition to robbery response training sessions that involve all credit union staff, guards, and local law enforcement, work with the guards and local law enforcement to create written guard duties and robbery response procedures. This will ensure that even though guards and employees may change, the quality of the response and their need to focus on life safety concerns will be the same at all locations.

Height Markers

There are no height markers at the exit from the lobby at any of your offices. Such markers will help robbery victims better judge the height of robbers leaving the lobby.

Recommendation: Install height markers at all lobby exits in all offices. Height markers are not only a good tool to use during a robbery, they offer a constant reminder and effective robbery response training tool for your staff. They also offer a deterrent to robbery as they send a message to the potential robber that your staff has been trained and they are ready.

Currency at Teller Stations

I discussed the currency exposure now at teller stations at each office. It appears your staff is making a good effort to conduct cash flow analysis and limit the exposure to only what's needed. I offer my compliments to your front line staff and operations managers.

Recommendation: Continue to reinforce the need for an on-going cash flow analysis both by operations managers and individual tellers. The goal is to limit currency as much as possible on the front lines. Make a discussion of "cash flow analysis" part of your on-going robbery training and awareness program. Constantly remind the frontline staff to limit their currency to only what's needed to provide good member service.

Spreading Teller Currency

I discussed the need to spread frontline currency between at least two locked containers at each teller station. For the most part tellers at each office are doing that. A few however suggested they monitor the cash flow so closely that they only keep what is actually needed.

Recommendation: There is nothing wrong with limiting the primary drawer to only what's needed and keeping all excess currency locked in a safe away from the counter. However, when staff change locations, they may not be able to judge their cash flow needs and excess currency will usually accumulate on the front lines. I recommend you make it a standard at all offices that front line tellers will use two locked drawers or containers to spread their front line currency exposure. At some offices tellers have two locked drawers and at others there is a locked drawer and locked tray and at others they have locked drawers and chutes that lead to locked under counter equipment. All help spread the exposure. Spreading front line currency both reduces your loss from a fast hit robbery and sends a message to the robbers that staff is well trained. The practice itself creates a deterrent to robbery.

Bait Money

I did not cover this in my 1999 report, however, I noted that "bait money" is not being used at any office. Bait money is money you can identify as coming from your credit union after a robbery.

Recommendation: I recommend you keep bait money in each teller drawer and in any change fund on premise. Simply record the denomination, bank of issue, serial numbers, etc of a number of bills so if they land in the hands of a robber, you'll be positioned to identify the currency as that coming from your credit union.

Dress for Success

Robbers are attracted to anything of value during the robbery. Expensive jewelry, personal credit cards and currency all make employees an attractive added target during a robbery.

Recommendation: Establish an employee dress code that discourages expensive jewelry or the carrying of personal property such as unnecessary currency or personal credit cards. This will better safeguard your employee's valuable personal property as well as reduce their attraction to the robber during an actual robbery.

Vault Door Time Locks

The currency vault door is equipped with a two-movement time lock. A recommendation was made in 2000 to use this important security feature. Time locks prevent the combination from being used during non-business hours. It is however still not being used.

Requirement: Consult with your security company and have them confirm that it's in operating order. Instruct credit union employees in its proper use and take advantage of this important security feature.

Defendable Zones

At all offices, it's important to establish defendable zones where employees can lock themselves in to summon police. As part of your "what to do during a robbery" training, identify defendable zones and develop a plan for employees to follow during any violent act on premises.

Requirement: At each office instruct guards to identify areas to which employees can retreat during a robbery or other violent act on premise. The area or "defendable zone" should have a lock on the door so employees can lock themselves in as well as a peep hole in each door so employees can see what's going on outside the room. Also, provide a telephone in the zone to call the police. The telephones in the defendable zone should not light extension lights on phones in the teller area. Guards should develop a signal to warn employees of a violent person on premise and instruct them how to reach the zone. Once employees are secure, guards should take planned action to deal with the violence.

Passwords

As in 1999 I noted passwords are not set to automatically force individuals to change them. Because Internet and hacker criminals are getting sophisticated, it's important to maintain tight password controls. Your plan at this time is to have them expire every six months. This according to the experts is too long a period to go without a forced change.

Requirement: I recommend you set them to expire no more than every 90 days. Instruct your management team to monitor this area and strive to set automatic changes every 30 days.

Currency Counting Machine

The currency counting machine is now in the teller area in clear view of anyone in the lobby. This creates an attractive target and motivation for a would-be robber.

Recommendation: The counting machine should be moved to the back office where currency can be counted out of sight.

JOHNSON CREEK BRANCH OFFICE

ROBBERY ANALYSIS

Money Safe

It appears that over 1 million dollars has been stored at this office during non-business hours. The currency is stored in the safe encased in concrete located in a concrete room with a rate of rise fire door. The concern is that the safe may or may not have a re-lock device in the combination. If not, the burglar could easily punch the combination with hand tools to gain entry.

Recommendation: Consult with your lock and safe provider to evaluate if a re-lock device is built into the door of the money safe. If not, have one installed. If a re-lock can not be installed, I recommend you limit overnight currency storage to 1 million dollars. As an added security feature, consider installing a door contact on the rate of rise fire door. Considering you already have an alarm reporting system to the police, the added door contact should be a low cost and simple security addition.

Hinge Pin Protection

The hinge pins on the rate of rise fire door leading to the money safe are exposed and could be removed to gain entry.

Recommendation: I recommend the hinges should either be spot welded so they can't be removed or be replaced buy hinges that have anchored pins. A lock professional can help implement this recommendation.

PLYMOUTH BRANCH OFFICE

Money Safe

During non-business hours, all currency on premise (over $1 million dollars) is stored in light metal under counter lockers. Under counter lockers were designed for basic access control. They were not constructed to be burglary resistive. A burglar can easily break into these lockers using common hand held burglary tools.

Requirement: All currency stored during non-business hours should be stored in a money safe that has a minimum UL burglary resistive rating TL-15. A TL-15 rated money safe has 1" thick solid steel walls and a 1 ½" solid steel door. It also has a UL rated re-lock device in the door to prevent punching of the combination.

Spare Key Controls

Teller spar keys are now stored in a locked key box. If a shortage occurs anyone with access to these spare keys will be a suspect.

Requirement: Similar to procedures followed in other offices, instruct tellers to first place their spare keys in a sealed envelop and sign over the seal before turning the key over to supervisors for storage. As long as the seal is not broken, the tellers can be held accountable for currency in their locked containers.

Risk Management Analysis
The First Credit Union of Houston Beach
Main and Two Branch Offices

Several commendable procedures and security measures were observed during the analysis. This report contains a review of physical conditions, practices, and procedures that represent increased elements of risk. The recommendations and/or requirements in this report are based upon statements made to us, as well as observed exposures and/or hazardous conditions. This report does not indicate that risks, not considered or observed, are adequately controlled.

COMMENTARY

This report may include recommendations and/or requirements. The definition for those terms is provided below:

A **recommendation** is our best advice of how to reduce loss, or the potential for loss, in a given area.

A **requirement** is a particular area of concern in which the credit union must comply with our solution, or negotiate an acceptable compromise for solution. Otherwise, underwriting action will be taken. The action could consist of lower coverage limits, higher deductibles, or a restrictive (exclusionary) endorsement.

In the written response you have agreed to submit, it is very important for the credit union to clearly indicate whether you will, or will not, adopt the individual recommendations and/or requirements.

MAIN OFFICE AND ALL BRANCH LOCATIONS

FOLLOW UP ON REPORT DATED MAY 2001

Some of the following is based on a review of recommendations made and management action taken after an on-site Risk Management Analysis was conducted at your main office (1906 Barber Drive) on May 2, 2002. A copy of the original report was mailed to the credit union May 3, 2002.

BURGLARY ANALYSIS

Vault Alarm

A vault alarm system was recommended based on your Safe Deposit Box service and the potential liability exposures should member' property stored in the boxes be lost. Because liability risks associated with safe deposit box services have increased since 1999, this recommendation has been elevated to a "requirement" in US credit unions. Based on the growing desire to sue, I believe credit unions in Great Britain should also elevate safe deposit box vault alarm systems to a "requirement."

Requirement:

According to your staff, plans are in place for the vault alarm to be installed in September when the vault is expanded. I compliment this action. Contact your CUNA Mutual Group Risk Management Specialist if you have questions relative to the recommendation in the 1999 report. I'm sure they can help clarify any questions.

Viewing Booth

Members are still allowed to view the contents of the safe deposit box inside the vault area. Many lawsuits are based on members being allowed to stay inside the vault to view their box contents.

Recommendation: When you expand and remodel the vault, provide a viewing booth outside the vault area. This will offer privacy to the member and significantly reduce your liability exposures.

Safe Deposit Box Guard Key

The credit union's safe deposit box guard key is stored in an open box in the vault. While this provides some protection against unauthorized access to the key, anyone in the vault has access to it. If a member claims their property was taken from the safe deposit box, your control over the guard key will be a major focus of any lawsuit.

Requirement: Store the guard key in the vault and in a locked container under the exclusive control of staff responsible for your safe deposit box service.

Stored Collateral

You now store loan collateral such as jewelry and other personal items in the safe deposit boxes in your vault. These items are appraised so their value is established. If you have a burglary, your credit union will be held liable for these items.

Recommendation: Discuss with your CUNA Mutual Group Account Relationship Manager what's covered and what's not covered. Store this property under dual control in one of the safe deposit boxes in the vault and keep a copy of the appraisals somewhere they will not also be taken during a burglary.

Perimeter Door Contacts

The door contacts on your perimeter doors still have exposed terminals. The burglar can easily gap these terminals (use a paper clip or any metal across the terminals) during business hours to circumvent their protection at night.

Recommendation: I recommend you install covers over the exposed terminals to discourage this type of circumvention. Such covers usually come with the component and should be available through your alarm installer.

Armored Car Service

I compliment your staff's use and knowledge of armored car services at all offices. As recommended in my 2001 report, it's also important that they continue to monitor the amounts transported and the liability coverage provided by the armored car service.

Requirement: Credit union staff at each location should review your armored car coverage limits in relationship to what's transported. Ensure the limits in your armored car service contract cover the full amount of all your cash shipments. In the alternative, you should limit your cash shipments to the amount of liability provided.

Robbery Training

Thank you for the opportunity to conduct robbery training at your main office. I noted during the analysis that such training is needed at all offices.

Recommendation: I recommend you consult with your CMG Risk Management Specialists. They can help you with your training needs. Set a goal to conduct such training at least every three months. Include all your guard services and local police in training. It is very important for all credit union staff, guards, and responding law enforcement to know what everyone is and will do before, during and after a robbery. Develop written procedures for your staff, the guards, and local law enforcement.

Post Robbery Trauma Training

Much can be done to assist robbery victims after a robbery.

Recommendation: As part of robbery training, include victim assistance training. For example encourage "non-judgmental" attitudes, victims to talk or vent. Help them deal with their guilt, fear, and sense of being out of control. Alert your Risk Management Specialist at CMG as soon as possible after a robbery.

Written Robbery Response Procedures

I compliment your use of armed and unarmed, uniformed and plain-cloths guards, and robbery alarm systems reporting to local police at each of your offices. Staff at each office indicated a general understanding of the guard's duties, practices, and procedures. Knowing exactly what guards and local law enforcement do and how they will respond to a robbery will help your staff feel more secure, more in control, and more prepared for robbery.

Requirement: In addition to robbery response training sessions that involve all credit union staff, guards, and local law enforcement, work with the guards and local law enforcement to create written guard duties and robbery response procedures. This will ensure that even though guards and employees may change, the quality of the response and their need to focus on life safety concerns will be the same at all locations.

Height Markers

There are no height markers at the exit from the lobby at any of your offices. Such markers will help robbery victims better judge the height of robbers leaving the lobby.

Recommendation: Install height markers at all lobby exits in all offices. Height markers are not only a good tool to use during a robbery, they offer a constant reminder and effective robbery response training tool for your staff. They also offer a deterrent to robbery as they send a message to the potential robber that your staff has been trained and they are ready.

Currency at Teller Stations

I discussed the currency exposure now at teller stations at each office. It appears your staff is making a good effort to conduct cash flow analysis and limit the exposure to only what's needed. I offer my compliments to your front line staff and operations managers.

Recommendation: Continue to reinforce the need for an on-going cash flow analysis both by operations managers and individual tellers. The goal is to limit currency as much as possible on the front lines. Make a discussion of "cash flow analysis" part of your on-going robbery training and awareness program. Constantly remind the frontline staff to limit their currency to only what's needed to provide good member service.

Spreading Teller Currency

I discussed the need to spread frontline currency between at least two locked containers at each teller station. For the most part tellers at each office are doing that. A few however suggested they monitor the cash flow so closely that they only keep what is actually needed.

Recommendation: There is nothing wrong with limiting the primary drawer to only what's needed and keeping all excess currency locked in a safe away from the counter. However, when staff change locations, they may not be able to judge their cash flow needs and excess currency will usually accumulate on the front lines. I recommend you make it a standard at all offices that front line tellers will use two locked drawers or containers to spread their front line currency exposure. At some offices tellers have two locked drawers and at others there is a locked drawer and locked tray. All help spread the exposure. Spreading front line currency both reduces your loss from a fast hit robbery and sends a message to the robbers that staff is well trained. The practice itself creates a deterrent to robbery.

Bait Money

I did not cover this in my 2001 report, however, I noted that "bait money" is not being used at any office. Bait money is money you can identify as coming from your credit union after a robbery.

Recommendation: I recommend you keep bait money in each teller drawer and in any change fund on premise. Simply record the denomination, bank of issue, serial numbers, etc of a number of bills so if they land in the hands of a robber, you'll be positioned to identify the currency as that coming from your credit union.

Dress for Success

Robbers are attracted to anything of value during the robbery. Expensive jewelry, personal credit cards and currency all make employees an attractive added target during a robbery.

Recommendation: Establish an employee dress code that discourages expensive jewelry or the carrying of personal property such as unnecessary currency or personal credit cards. This will better safeguard your employee's valuable personal property as well as reduce their attraction to the robber during an actual robbery.

Vault Door Re-lock Device

There is some doubt as to whether or not a "re-lock" device is built in to the currency vault door. The re-lock device does what it says, it re-locks the door if the burglar attempt a punch job on the combination.

Requirement: Consult with your lock company and have them confirm there is a re-lock device in this vault door. If not, have one installed. An alternative recommendation would be to purchase a TL-15 rated money safe for currency, member collateral, and other valuable property storage.

Defendable Zones

At all offices, it's important to establish defendable zones where employees can go, lock themselves in and summon police. As part of your "what to do during a robbery" training, identify defendable zones and develop a plan for employees to follow during any violent act on premises.

Requirement: At each office instruct guards to identify areas to which employees can retreat during a robbery or other violent act on premise. The area or "defendable zone" should have a lock on the door so employees can lock themselves in as well as a peep holes in doors so employees can see what's going on outside the room. Also, provide a telephone in the zone to call the police. The telephones in the defendable zone should not light extension lights on phones in the teller area. Guards should develop a signal to warn employees of a violent person on premise and instruct them how to reach the zone. Once employees are secure, guards should take planned action to deal with the violence.

MONROE STREET BRANCH OFFICE

ROBBERY ANALYSIS

Camera

The surveillance system at this branch locates the monitor in the manager's office. While this does allow the manager to observe what's going on in the lobby, locating it so members standing in the lobby would increase its robber deterrent value. Locating a monitor off premise would provide even more deterrent value

Requirement: Position the monitor so those waiting in the lobby will be able to watch what's being recorded. Discuss the possibility of locating a monitor in the Mall security command center. Use "security integration" principles and explore locating a monitor at your other branch office and one of theirs in your branch. The goal is to send a message that someone located at a distance and in a safe area will be aware and positioned to effect an appropriate response. Discuss security integration principles with your CMG Risk Management Specialists.

Armed Guards

I compliment your use of armed and unarmed guards both uniformed and in plain clothes. This creates an important deterrent to robbery. My concern is both guards are positioned within the teller area or what's considered you primary "defendable zone." During a robbery they might easily be overpowered and their protective value compromised.

Requirement: The goal is to separate the guard with one on-premise and one off or at a distance so they can respond during a robbery to summon police or other appropriate back up protection. Another important deterrent would be to locate one guard outside the lobby entrance to clear members into the lobby.

Guard Communications

At this time guards have no way to communicate either with each other or with mall guards and local law enforcement.

Requirement: Provide all guards with radios that link them to appropriate law enforcement officials. Ideally, that includes mall security as well as local law enforcement. Guards should be trained on radio use and appropriate law enforcement response procedures.

Office Floor Plan

The floor plan at this branch affords little distance from the teller counter to the exit. This benefits a robber as they can easily control everyone in the lobby as well as quickly escape.

Recommendation: I recommend you change the floor plan to increase the distance from the counter to the exit. For example, evaluate the floor plan at other financial institutions at the mall and note the distance they've created. Also note the location of employees, especially those behind shoulder high partitions. A robbery deterrent is created when the robber might see employees but not be able to know what they are doing from the neck down. The employee having some "cover" could be activating an alarm or an intercom to the police. Discuss your floor plan with your CMG Risk Management Specialists. They can share other "Crime Prevention Through Environmental Design" Risk Management principles that might help.

Lobby Bullet-resistive Barriers

The barriers at this branch over the teller counter are not bullet resistant. This is very important from a liability standpoint. You do not want to raise you employee's security expectations beyond what you have provided.

Requirement: Communicate this to all your employees so they know the barriers are only designed to be for access control to the teller area. If you elect to install bullet-resistive barriers, the barriers should be UL listed and the installation done by a qualified installer. Barrier materials would be needed both below the counter as well as above the BR glass. Also, air circulation and voice communication systems would have to be appropriate for the teller area. Consult with your CMG Risk Management Specialist for more information.

Robbery Alarm Actuators

Some robber alarm actuators are located at the teller counters and another at the managers desk. I'm not sure if one was in the break area or not.

Recommendation: Depending on your future floor plan, additional actuators such as in the break area should be installed. Portable actuators are available, I believe through your security company. Portable actuators have the advantage of being used anywhere near the credit union. They therefore off some added deterrent value and should be considered.

Alarm Warning Lights

I did not confirm whether or not warning lights were located in the break room.

Recommendation: Use the same very good approach to alarm warning lights you used at the main office and install alarm warning lights both in the break area and managers office. A light in the manager's office will be especially important if you move the CCTV monitor. The goal is to alert staff in the break room to a robbery in progress so they don't inadvertently walk in and frighten the robber.

Safe Alarm - Extortion

The money safe you have provides excellent burglary protection for the currency you're storing during non-business hours. From a burglary perspective a safe alarm is not needed. However, considering you have a robbery alarm with a reporting circuit to the police, adding a door contact on the money safe and wiring it separate from other alarms would give you one added level of protection against someone forcing staff to open the safe. The cost for this added benefit might be very small.

Recommendation: Consider adding a door contact to your money safe the next time you upgrade your alarm system. Controlling who has a shunt key to this safe alarm will help discourage an extortion attempt.

Window Covering

Window covering can be good and bad. Set a goal to provide as much view of the lobby area as possible day and night and a controlled view of the manager's office during business hours. Allowing the public to see into the lobby helps discourage robbery while limiting a view into the manager's office during the day also discourages a potential robber.

Recommendation: Provide a clear view into the lobby by removing any unnecessary decals and all window' covering both day and night. Open the drape in the managers office and place a motion light (activated by movement in the area) on the safe. Ask guards to be alert to any light on in the manager's office during non-business hours. Note there is a suspended ceiling in the manager's office that might lead to other mall tenants. The open drapes and motion light will help detect anyone entering the manager's office via the suspended ceiling.

WOLDT'S CORNER BRANCH OFFICE

Money Safe

According to cash records at this location, over $650,000 is stored in a ¼" cash locker in a record vault. Neither the cash locker nor the record vault was designed to protect against forced entry. A burglary could easily enter both using simple hand tools.

Requirement: Purchase a TL-15 rated money safe for all currency storage during non-business hours at this branch. The TL-15 safe provides solid steel walls 1" thick and a door 1 ½" thick. The door also comes equipped with a re-lock device. A standard in the credit union movement established in 1971, requires all credit unions that store over $500US during non-business hours to store the exposure in a money safe that carries at least a UL TL-15 rating.

Example – Memo to File

- **Example of a PC based "memo to file" If filed electronically use bond contract number ending with an "M" This is an internal document used to pass on information such as loss history not included in a claim or a comment made by a dependable source. Stick to the facts using dates, who said what, where it was said, etc.**

To: Corporate P&C Risk Management
Corporate P&C Underwriting

From: Richard A. Woldt

Subject: [Click and enter credit union name]
[Click and enter credit union contract number]

Assets: [Click and enter credit union assets]

[Click here to begin the text of your memo]

Bond Renewal Survey Examples

Insert Examples Here!

Section V

Risk Management Support Systems

Section V

Risk Management Support – Research and Development Materials

1. WWW.cuanamutual.com **– Set up your mycuanmutual page to access the CMG "Loss Prevention Library and other CMG resources.**

2. WWW.RMLearningCenter.com **For trauma management training, contingency planning, violence in the workplace and other risk management training resources to include focused Risk Management workshops, presentations and links to security related web sites and security equipment manufactures.**

3. **Brochure List:** The brochure list on next pages is designed to be faxed to credit unions so they can request brochures of interest. This could be edited to fit Great Britain and the inventory of brochures stored in country.

Brochure Listing to fax to credit unions. Consider this for Great Britain based on brochures available.

CUNA Mutual Group
Risk Management T9-6
Post Office Box 1084
Madison, WI 53701-1084
www.cunamutual.com for additional brochures

800/637-2676
Fax: 608/231-8987
We have the following brochures available.
Please check desired brochures.

4	Form #	Brochure
	CRM-135	5 Details Which Identify Criminals
	CRM-136	What To Do If You Are Robbed
	CRM-146	Managing Risks Of Member Forgery And Fraud
	CRM-147	Audit Control Procedures
	CRM-151	CU Currency Vault Security Specifications
	CRM-154	RM Security Guidelines For ATM Systems
	CRM-205	CU Audit Procedure: Detection Of Fictitious/Unauthorized Loans
	CRM-220	Burglary Prevention Methods
	CRM-230	Share Draft Kiting - Teller Card
	CRM-245	Wire Transfer Security
	CRM-256	CU Business Lending Guidelines
	CRM-258	Business Lending Considerations
	CRM-259	Post Robbery Trauma
	CRM-260	Setting Share Draft/Checking Guidelines
	CRM-261	Development Of A CU Fraud Policy
	CRM-262	Record Storage Program
	CRM-263	Managing The Risk Of Robbery
	CRM-263A	To Catch A Thief
	CRM-268	CU Internal Control Considerations
	CRM-272	Managing Risks Associated With Safe Deposit Box Services
	CRM-279	CU Office Safety
	CRM-286	Planning To Survive A CU Disaster
	CRM-292	Credit Unions And Risk Management
	CRM-293	Real Estate Loans Guidelines
	CRM-303	Brochure List
	CRM-326	Fidelity Bond: Underwriting Options
	CRM-335	CU Ergonomics
	CRM-336	Cellular Alarm Installation Specifications
	CRM-338	Managing The Risks Of Indirect Lending
	CRM-339	A Credit Union's Guide To Managing Consumer Lending Risk
	CRM-354	Actions To Take After A Robbery
	CRM-356	Managing Extortion Risks

	0281-P1021	What Every Director Should Know
	0281-P1066	Stop Plastic Card Loss
	0281-P1103C	A Checklist For Evaluating Your Card Programs
	0281-P1115	Risk Management Activities
	0281-P1135CF	Check Fraud Self-Assessment Checklist
	0281-P1135DP	Disaster Protection Self-Assessment Checklist
	0281-P1135EC	Electronic Commerce Self-Assessment Checklist
	0281-P1162	Telltale Signs of Check Fraud

Credit Union Risk Management

Security Officer Checklists & Manuals

Each credit union should customize their own "Security Officer checklist and use it to ensure appropriate security equipment is installed, regularly tested and all credit union employees are properly trained. Training, at a minimum should include what to do before, during and after a robbery, cash handling and storage procedures, and recommended internal controls. Specific attention should be given to the proper use of access controls such as keys, combinations, pass words and access codes. Security lighting should be discusses as well as the need and proper use of surveilance systems.

Credit Union Risk Managers should start identifying exposures to loss. For example, identify the total maximum currency on premise during the day and stored at night. Once all exposurers to loss have been identified, you can then evaluate the physical security, alarm protection, policies and procedures used to safeguard against loss.

SECURITY

Risk Manager/Security Officer: *The Board of Directors will designate a Credit Union "Risk Manager" often referred to as "Security Officer" who will be responsible for the installation, testing and maintenance of security equipment, as well as security policies, procedures, and training at each credit union location.*

Credit Union Risk Management Program/Guide: *The Credit Union Risk Manager will customize a security program to include maintaining a written guide for each credit union location. The scope of our security program will take into consideration maximum currency exposures, our asset size, member services, and the physical location of each office. The Credit union Risk Manager will consult periodically with Risk Managers at CMG to ensure we are in compliance with recommend security standards.*
To ensure credit union security equipment is properly used and all credit union security policies and procedures are followed, Credit Union Risk Managers should develop security checklists, appropriate to each credit union office, and self assess locations at least annually. Following is a sample checklist used by a large US credit union. Note this is a fluid document designed to grow with the credit union. Some questions repeat because larger credit unions will have similar concern in different departments. For example, cash handling questions might be used by teller operations as well as in the ATM department. Customize your checklist using input from the your entire management team. Risk Managers at CMG can help your credit union customize this important security self-assessment tool.

Sample Security Self Assessment Check List

Identify Major Exposures to Loss

Credit Union: _____
Physical Address: _____
Date Updated: _____

1. Currency Exposures and Security Equipment at this location:
2. Maximum currency exposure during business hours: $_____
3. Maximum currency per teller station: $ _____ Number of teller stations: _____
4. Maximum currency exposure during non-business hours: $_____
5. Maximum other cash items (Blank Traveler Checks, Collateral, etc.) $ _____
6. Burglary resistive rating of safes/vaults used to store currency during non-business hours:
   _____
   _____
   _____
7. Alarm components protecting the safe/vault:
   _____
   _____
8. Alarm components protecting the building perimeter or areas:
   _____
   _____
9. Other alarm security features such as line security protecting reporting lines to the police:
   _____
   _____
10. Describe surveillance system(s):
    _____
    _____

Sample Checklist Questions to Evaluate Credit Union Security Equipment and Procedures

1. Safety and Loss Prevention Plan

   a. Protection for Personnel

      1) Training sessions are held for all directors, committee members and employees covering the precautions and procedures of loss prevention. Frequent refresher sessions are held for all employees.

   b. Loss prevention procedures are in writing. Each director, committee member and employee has a copy.

   c. Directors, committee members and employees are instructed not to talk carelessly in public about credit union business, particularly about cash handling procedures.

   d. All employees are instructed not to play hero and not to offer resistance to hold-up men.

   e. Bank lodgments are carried by two employees if over ($ _____) or a police escort is provided.

f. The police are to be alerted if suspicious persons or loiterers frequent the area of the credit union office.

g. Risk Manager/Security Officer duties:

1) Maintain effective key control system to include storage of spare keys and combinations.
2) Confirm all currency is stored in appropriate burglary resistant containers and all vital records are stored in fire resistant containers.
3) Complete or review bank reconciliation to determine they are timely and there are no uninsured lodgments in transit.
4) Review "daily evening security check" made by designated employees.
5) Make periodic cash drawer audits to ensure tellers are conducting a cash flow analysis and spreading their frontline currency exposures.
6) Develop and conduct periodic fire drills.
7) Confirm blank credit union checks are properly inventoried and stored.
8) Remain alert to situations that might result in a loss to the credit union and/or its personnel and report concerns to upper management.
9) Confirm the credit union disaster recovery program to include the off site storage of vital information is up to date and appropriate for all credit union operations.
10) Consult with CMG Risk Managers to develop a continuing education program focused on Credit Union Risk Management and security for financial institutions.

2. Protection of Premises

a. Instruct all employees to not be lured outside of the credit union office by unusual disturbances, leaving the office unprotected.

1) A security check is made daily at the close of business.
2) Fire drill procedure includes a check of premises by assigned management or supervisory personnel.

b. Messengers, maintenance persons, and delivery persons are handled at reception desk. Identification is requested when necessary. Unauthorized personnel are not allowed in work areas.

c. Combinations to the vault or safe are subject to change following changes of employees.

d. At night, designated security lights are left on and draperies remain open to afford a view of the lobby area by passing police.

e. Door keys are marked "NOT TO BE DUPLICATED UNDER PENALTY OF LAW" and controlled by the credit union management.

- Exterior door keys to credit union owned buildings are assigned to select personnel.
- Interior keys are assigned to employees having a need for access to specific areas.
- Duplicate keys are stored in sealed envelopes with signatures over the seal.
- Access controls (keys and combinations) are divided so more than one person is needed to get from the parking lot to stored currency during non-business hours.

f. Locked, fire-resistant files are used to store all vital records such as loan files.

g. Appropriate multi purpose fire extinguishers are properly mounted throughout each office and all employees are trained in their use.

3. Protecting Currency

a. All employees are trained to conduct a “cash flow analysis so only enough currency to provide good services is kept on hand.

b. All excess currency is lodged at the end of the day.

c. Only a working fund is kept in the counter drawer for each teller. Other cash is kept in the safe.

d. All checks are stamped "FOR DEPOSIT ONLY" <u>immediately</u> upon request.

e. All currency is promptly placed in the teller counter drawer, to include bait money and money in bill traps designed to activate the robbery alarm.

f. A small amount of "bait" money is placed in each cash drawer. The serial numbers, series year, bank of issue and denomination are kept in a separate file.

g. Voided checks are marked "VOID" to help stop negotiation.

h. Messengers are not permitted to make other stops when transporting cash.

i. A duplicate copy of the deposit slip is made for all deposits.

j. Each member is required to present a valid ID for withdrawal purposes.

k. Surprise cash counts, are made by office managers.

l. Bank reconciliation(s) are checked by management and the examiner.

m. Tellers are instructed to use only their cash drawer. No employee is to have access to another cash drawer unless authorized.

n. Two employees acting jointly verify all receipts through the mail and the night depository.

o. The night depository has a fish and trap resistant head and dual locking container.

p. Cash withdrawals are handled on the same basis as checks: the signature is normally checked against the signature card before disbursing cash.

q. Change making should be limited to one simple exchange. Palming (a practice of keeping a bill during several exchanges) can cause a teller to be shorted.

r. Blank traveler's checks are stored in burglary resistant safes, blank credit union checks and money orders are inventoried and stored in a locked vault. Traveler Check records are audited by the Supervisory Committee and Operations Manager.

s. Bond coverage is maintained and reviewed semi-annually by management and the board of directors.

4. Hold-up Precautions (Employees)

a. While a hold-up is taking place, follow these procedures:

1) Remain calm and carry out the robber's orders without argument.
2) Be observant. Notice details of speech, mannerisms, appearance, firearms, and make of car and license number.
3) Compare the robber's height with some object in the office, so that you can describe him/her accurately.
4) Attempt to include bait money with money taken by the robber. It helps identify stolen money.

b. When the robber leaves:

1) Note method and direction of escape.
2) Alert the president/manager to immediately notify local police.
3) Don't touch; move or disturb anything until the police arrive.
4) Instruct employees and all witnesses to complete pre-printed robbery description forms or have them write down all they saw. Collect these statements before allowing them to discuss the robbery among themselves.
5) Keep curious people away.
6) Give the police the list(s) of bait money.
5) If the robber used a note, turn it over to the police. Do not handle it any more than is absolutely necessary.
6) Get the names and addresses of all witnesses, including passerby, who observed the robber leaving. Protect your witnesses; give their names only to the police.
7) Do not tell the press or outsiders about money that was overlooked or point out that money was missed. Only designated upper management is authorized to make a statement to the press.
8) Notify the bonding company and request proof of loss forms.
9) Notify CMG Risk Managers.

4. Urgent Building Safety Problem

In the event of an urgent building safety problem:

a. Notification will be given to the Credit Union President/Manager or Risk Manager.
b. Fire or bomb evacuation procedures will be followed.
c. Note any unusual objects, container, or signs of danger when leaving your work area. Be alert all the way to the meeting point.
d. After being assured it is, secure currency that might yet be unsecured and cooperate with law enforcement and other emergency response personnel.
e. You may be advised to report to a specified area to be recalled when safety is assured.

5. Fire Drill Procedures

    a. Tellers carry cash drawers to vault, or lock cash drawers.

    b. Loan granting personnel place loan folders and supporting documents in safe and fire resistive files.

    c. Accounting personnel place vital records in fire resistive safes.

    d. Put EDP processing report in fire resistive safe, along with check forms and other cash transaction information.

    e. Lock files, drawers, turn off lights.

    f. Spin all combination locks and lock all safes and fire resistive files.

7. Evacuation Route

    a. Employees should move quickly and quietly to the nearest exit.

    b. Use alternate exit if one should be locked. Move quickly but do not run.

    c. Report to the meeting point for roll call.

    d. Review all site specific instructions for fire evacuations. Discuss them with fellow employees.

8. Check Out List to be Used at Close of Business

    ☐ Music system turned off?

    ☐ Loan files in vault?

    ☐ Money orders in safe or fire proof files?

    ☐ All machines covered?

    ☐ Traveler' checks in burglary resistive safe?

    ☐ Are all doors locked at closing?

    ☐ All currency locked in burglary resistive safe or vault?

    ☐ Lights off except over safe door?

    ☐ Straighten teller area and is all confidential information locked in appropriate container?

    ☐ Is microfiche in fire resistive container?

    ☐ Are deposit bags in burglary resistive safe/vault or is night deposit at the bank?

☐ Are all containers to include burglary and fire resistive containers locked?

☐ Are draperies open so police can see into the lobby area?

Risk Manager/Security Officers' Initials: _____

Credit Union Risk Management Manuals

There have been many efforts to provide credit unions with site specific Risk Management manuals. It usually results in the credit union customizing a manual from a checklist such as the checklist discussed earlier. Or, credit unions compile a binder of risk specific brochures published by CMG, leagues and trade associations. This is usually preferred as it allows credit unions to easily keep the manual up to date. Credit union techology and risks change constantly so brochures on risk areas also change quickly. Having manuals stored electronically helps in updating but it's not a cure all. ***An important part of the Credit Union Risk Managers' written duties should be to annually update all security policies and procedures.***

Filed in this section are samples of Credit Union Risk Management manuals. Scan them into this manual as a word document so CMG Risk Managers might use them as a template to develop a manual for credit unions in Great Britain. I recommend, however, using the "checklist" approach, outlined earlier in this manual first, as the site specific checklist will better focus Credit Union Risk Managers on risks that are most important to the credit unions, CMG, and CUNA MUTUAL GROUP in Great Britain.

File Samples of Credit Union Risk Management Manuals here!