Issue 6 | November 2013

BEST OF

Network Compliance Teacher

Compliance News and Tips from Credit Union Compliance Officers
sponsored by CU*Answers AuditLink

In this Issue...

Editor's Corner

It has been a busy 2013 for compliance officers so we decided to give your authors a bit of a break to help them catch up on all the new mortgage rule requirements. The team here at AuditLink has been busy as well finalizing the specifications for the changes to CU*BASE and assisting our programming staff as we wade through the many lines of code changes.

So for this edition of the Network Compliance Teacher, we thought we would give you a second peak at what we believed to be the best of the first year of articles that came out of our network of aspiring authors.

On a side note…. With all the changes required by the new mortgage rules the PolicySwap site (http://policyswap.cuanswers.com/) has been getting deluged with new policies and registrants. I would encourage you to go out and visit if you are struggling through your own.

Jim Vilker, NCCO
VP of Professional Services
CU*Answers

Get Involved with the Network Compliance Teacher!

Have something to contribute?

Want to write an article for a future Network Compliance Teacher Issue?

Have a topic to suggest for a future issue?

We're looking for compliance officers like you to contribute!

Contact AuditLink at auditlink.cuanswers.com

The Network Compliance Teacher is a collaboration of compliance minded Credit Union Professionals like you from throughout the cuasterisk.com network.

The Network Compliance Teacher is published quarterly. Current and previous issues are available for download from the AuditLink website at http://auditlink.cuanswers.com.

AuditLink
CU*ANSWERS Management Services

6000 28th Street SE
Grand Rapids, MI 49525
(800) 327-3478
auditlink.cuanswers.com

Proud Member of the cuasterisk.com Network

Managing High-Risk Accounts

Amanda Craig
Compliance Officer
Honor Credit Union

Member Service

Determining account risk when opening a new account is the responsibility of member-service team members. Compliance and audit staff who perform ongoing monitoring of high-risk accounts rely on frontline staff to gather accurate and useful information.

Determining Account Risk When Opening a New Account

There are many factors to consider when rating a new account such as whether the account is for a new or existing member. Existing members have an established relationship and have already proven themselves to your credit union. Other factors may include residency, how/where the account was opened, how it was initially funded, and the member's profession and business activity. This list is not all-inclusive and should be tailored for your credit union's needs.

Residency: A non-resident alien is a greater risk than a US person or resident alien.

Account Opening: Was the account opened in person with all parties present and were you able to verify documentary ID or was the account opened online or via another channel where non-documentary information was relied upon to form a reasonable belief that the person is who they say they are?

Opening Deposit: Was the account opened with cash, payroll check, personal check, cashier's check, or by other means? The varying types of initial funds create different risks for the credit union. Unfortunately, we have all seen account-opening checks go bad such as when a personal check is returned because the account is closed or when a cashier's check is found fraudulent.

Professional Service Providers: There are certain professions that pose a greater risk to your credit union. Examples include doctors, lawyers, accountants, insurance agents, real estate agents, travel agents and politically-exposed persons. A member who falls into one of these professions doesn't necessarily have a high- risk account, additional risk factors must be considered in order to determine a member's level of risk.

Nature of Business Activity: There are business types that require more monitoring than others since they have a greater potential to be a money-service business. Examples include convenience stores, restaurants, retail stores, liquor stores, charity or non-governmental organizations and auto dealers.

A best practice is to complete the new member's risk rating, along with monthly anticipated account activity and a Member Identification Program card for an overview of the new-member relationship. One helpful tool CU*BASE Gold offers within the Updated Membership Information screen is the Due Diligence Monitoring Level, which needs to be completed after determining the risk rating. Since there are no pre-defined fields, each credit union may choose to assign different meanings to each value. The new-account team member's duties don't end once they've updated the account with a risk rating. . The compliance and audit staff have reports to review, but they can't do it on their own; they rely upon feedback from frontline staff who are the first to notice suspicious or unusual account activity.

Ongoing Monitoring of High-Risk Accounts

The Insider Audit/Due Diligence Report allows compliance and audit staff to review high-risk account activity such as a previous SAR filing and configuration exceptions (i.e. an A2A set above a standard limit). This monthly report allows you to review transactions and file maintenance to determine if any recent account activity is unusual or suspicious. As your membership grows, you may find your high-risk accounts growing. Review initial-account risk-rating levels and reassign as needed. An account opened online or by phone may have been deemed high risk due to several risk factors, but has account activity been in line with the expected account activity for several months with no exceptions? The account can be reassigned to a lower due-diligence monitoring level. In short, ongoing monitoring is essential to any fraud program as it protects the credit union and the member.

NCT

Regulation CC and Electronic Hold Groups

Jessica Hillborg
Compliance and Internal Audit
Frankenmuth Credit Union

Teller

Regulation CC requires disclosures to be made to members stating when funds from their deposit will be available for withdrawal. Recently, there was a change to the regulation that now requires $200 of the deposit to be made available the next business day following the deposit. The entire amount of the check must be made available by the second business day following the deposit. There are exceptions to this rule, however, and an extended hold of seven days is applied if one of the exceptions is met. New accounts (within the first 30 calendar days) also have special rules that can extend the hold to as much as nine business days. It is imperative to properly disclose to the member when the funds from the deposit will be made available as well as to provide them with reasoning if an extended hold is placed.

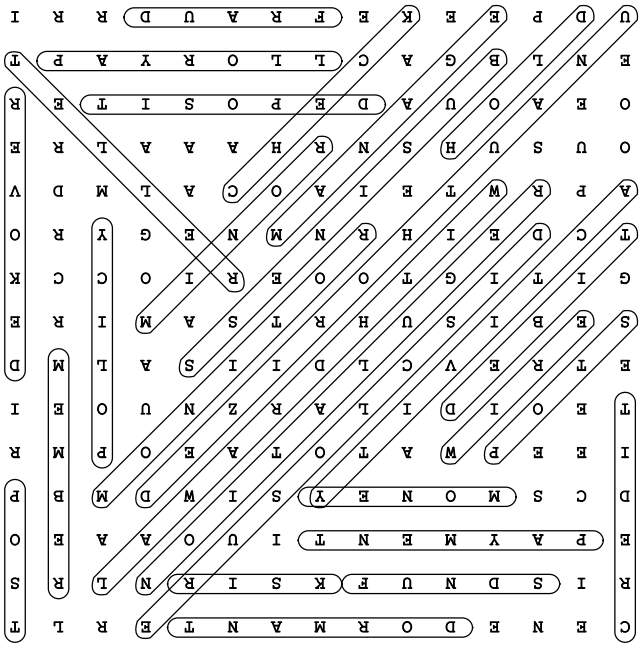
ATM deposits have their own set of rules concerning funds availability. Deposits made into a proprietary ATM have the same availability schedule as deposits made in person (two-day hold with $200 made available the next business day). However, deposits made into a non-proprietary ATM have a longer hold period of five business days. It is each individual credit union's decision as to whether or not they decide to impose a hold on ATM deposits.

Through the CU*BASE platform, an electronic-deposit hold configuration can be set to determine how long a member's deposits will be held. These holds are applied across the entire membership, and exceptions can be made from there. Using MNCNFD #20-Electronic Deposit Hold Config, it is now easy to set up an exception that will apply every time a certain member makes a deposit. This way, members in good standing can be set up for immediate availability if the credit union wishes to do that. For members who continually make ATM deposits, using this menu to its full potential will remove the need to call the credit union each time a hold needs to be released. This functionality allows credit unions to reward good members by not placing a hold on the deposit each time one is made. As always, the member can be removed from the "member in good standing" hold group if the member abuses that privilege.

Once the hold groups are set up and defined through MNCNFD #20, the hold group for individual members can be changed using MNUPDT #1-Update Membership Information. Anyone who can update member information can then change the hold group to allow members to have an electronic-hold-group configuration that is different from the default. The key to successfully using the electronic-deposit hold groups is to accurately define each group and apply it in the situations where it is necessary.

For more detailed information and step-by-step instructions, refer to the booklet, "Electronic Deposit Holds and Member in Good Standing Configuration," in CU*BASE online help (http://cuanswers.com/pdf/cb_ref/E-MbrinGoodStanding-ElecDepositHolds.pdf#2011-12-28).

NCT



ACH - Stop Payments vs. Unauthorized

Marsha Sapino, AAP
AuditLink Associate
CU*Answers

Member Service

Scenario One
Mary Member contacts your credit union informing you that last month an ACH debit hither account from a company she's never even heard of. Having never authorized this debit, Mary wantsher money back as well as assurance that this company will never debit her account again.

If you've ever experienced this scenario before, you know how confusing it can be to know the right steps to take.

In the above scenario, the first step is to make sure this will be a timely return since the member is claiming that the debit was unauthorized. According to ACH rules, the member has a 60 day right-of-return from settlement date to have an ACH item returned as unauthorized.* In this case, the debit posted to the member's account last month, so the item may be returned timely.

In addition, because this is an item that has already posted to the member's account, a "Written Statement of Unauthorized Debit" (WSUD) is to be obtained and the debit returned by the credit union to the Originating Depository Financial Institution (ODFI) as an R10-Customer Advises Not Authorized. Lastly, the member is to be credited their funds back.

Now in a perfect world, the item should not be re-initiated by the ODFI. When an item is returned as unauthorized, it should not be resubmitted. But we all know that this is not always the case. A WSUD is good for ONE item and is only used to return an item that has already posted to the member's account. It should not be used to stop any future debits of said item. Either the credit union can take a stop payment from the member to stop any and all future debits from the company or the member can wait to see if the company debits them again, and at that point, a new WSUD will have to be obtained and the new debit returned as unauthorized. As an added note, the credit union can now file a rule-violation notice against the ODFI for resubmitting an item that was previously returned as unauthorized.

Scenario Two
Mark Member contacts your credit union telling you he's worried that a company to whom he gave his account information over the phone will debit his account for a service that he called back to cancel just minutes after signing up for the service.

As a credit union employee, you've probably experienced this scenario before and may have wondered what steps to take next: do you take a stop payment or request a WSUD?

In this scenario, the member has two options. He can either place a stop payment on the item or, if he doesn't want to pay the stop-payment fee, he can wait to see if the company does debit his account. Because the member contacted the company to cancel prior to the date of the debit, he now has return rights under the ACH rules. If, during the 60-day right-of-return window, the company debits the member's account, the member can fill out a WSUD and the debit can be returned as an R07 – Authorization Revoked by Customer. The WSUD must document that the member contacted the company to revoke the authorization BEFORE the date of debit.

Again, the ODFI should not re-initiate the debit at this point, but there is always that chance. The member in this scenario has the same options as the member in scenario one.

One last note to keep in mind about stop payments.In 2010 the stop-payment rule was updated to reflect the removal of the six-month expiration. As a result, members can now place a stop payment on an item either for a one-time entry or indefinitely. If they haven't been already, your CU policies should be updated to reflect this change. When placing an indefinite stop payment for a member, the expiration date on the record must be changed to all 9's.

NCT

*Reg E states that the member has 60 days from statement date to dispute an item. Stay tuned for Edition 4 of the Network Compliance Teacher newsletter for information on error resolution Reg E style.

Dormant Accounts

Terri Urbanek
Internal Financial and Operations Auditor
Community Credit Union

Internal Auditor

Are your dormant accounts golden eggs waiting to hatch? Will they hatch good or evil?

Credit unions who do not have a program in place to monitor activity on dormant (inactive) accounts may find themselves facing multiple claims of embezzlement. To avoid this potential fraud, your credit union can use the CU*BASE system to monitor the dormancy status of accounts.

While every state defines dormant accounts differently, an account is typically considered dormant if there have been no transactions on the account for a number of years. The Dormant Member Processing Configuration (MNCNFA #11) allows you to set dormancy parameters indicating when an account is dormant and also to set the escheat flag, according to your state's requirement, to forward abandoned funds. This is also the screen in which you can set the fee amount and frequency to charge and the controls for exclusions or fee waivers.

Your first step in monitoring the dormancy status of accounts is to establish your level of transaction risk, which is the current and prospective risk to earnings and capital arising from fraud or error, the inability to deliver products/services or maintain a competitive position. You can do this with a review of the number of dormant accounts. Start with a review of the total number of dormant accounts you have. From MNUPDA, #9, select the Summary F15 button. The Summary provides an overview of all funds in dormant accounts according to the length of time the member has been on the dormancy list. Typically your risk lies in withdrawals from dormant accounts. Deposits into dormant accounts may also present some risk if an employee is using the account to move misappropriated funds out of the credit union. Next, determine if your greatest risk lies with small-dollar withdrawals, large-dollar withdrawals, or any transaction type. A credit union should give special attention to dormant accounts that are labeled with wrong address flags and to dormant accounts with sudden activity.

Now that you have the parameters established and have determined your level of risk, you will need to monitor activity using MNAUDT #5 or MNUPDA #9. If an account was suspended or is showing No Active Membership, determine what activity occurred and whether or not it requires further investigation. Withdrawal transactions can be verified by reviewing a copy of a signed transaction receipt and comparing the signature with the member signature on file. If signatures seem reasonably similar, make a note in the tracker that the transaction was reviewed. If signatures are not similar, make an attempt to notify the member by mail and ask them to make contact with the credit union to confirm the activity. Deposit activity can be verified with reviews of the item deposited, deposit slips, or contact with the member.

When you have completed your review of transactions, you can determine if the account should be reinstated as dormant (i.e. the activity was the posting of a fee) or if the account was reactivated and should be deleted from the dormancy file.

Don't forget that you also need controls in your branches. When you turn dormancy monitoring on, the system will automatically place a comment on a membership that has reached dormancy status. This alerts member-service team members to be especially careful in performing a transaction on the account. Appropriate member identification is critical before any transaction is completed. Branch team members who work with a membership that is dormant should use an appropriate process to identify the person requesting to conduct a transaction and explain to the member what dormancy means and how a membership can be reactivated.

Preventing Fraud in the Accounts of Decedents, Minors, and Other Fiduciaries

Amanda J. Smith
Messick & Lauer, P.C.

Member Service & Back Office

Decedent, minor and other fiduciary accounts, such as those subject to powers of attorney, are particularly susceptible to fraud. While some of these instances of fraud may result from an ignorance of the law on the part of the person with whom the credit union is dealing, many times they are purposeful evasions of the law and attempts to circumvent other beneficiaries. While I do not suggest that the credit union perform a full legal evaluationfor every such account, it can put in place certain policies and procedures to minimize the risk associated with these accounts.

Here are a few scenarios to put the risks in context:

A woman comes into a branch with only a copy of the death certificate of the member and a will that states she is the executrix of the estate. She wants to withdraw all of the funds from the decedent member's accounts. Can she? Probably not.

A co-agent appointed through a power of attorney comes into a branch without the other co-agent to withdraw the funds from the principal's account. Can he? Maybe.

The grandmother of a minor child comes into a branch with a letter from the mother of the minor child stating that she appoints the grandmother the guardian of the minor child. She would like to withdraw the funds from the minor child's account. Can she? Probably not.

The definitive answers to these questions and all questions involving decedents, estates, and fiduciaries are guided by state law, and therefore will vary. The law is voluminous and can be difficult to handle, but the following steps will help the credit union better manage these accounts.

First, the credit union should have detailed polices in place for use when dealing with these accounts. While it is impossible to write policies for every set of circumstances that may occur, the credit union can write policies to help guide its employees in the most common situations encountered in the branches. It may be helpful to work with local counsel when drafting these policies to be sure that they are in line with current state law, and they should be revised by counsel, as necessary, to reflect any changes in the law.

Second, the credit union should educate the individuals who are handling these accounts. These individuals should know the credit union's policies with regards to these accounts and should also be apprised of the law in this area. For example, these individuals should know the rules and documents necessary to confirm the authority of an executor and an agent appointed through a power of attorney. Good resources for education are the classes offered to attorneys and paralegals. There are webinars and teleconferences which offer a high level overview of these areas of the law that can help educate the credit union employees. Most states do not require a financial institution to do independent investigation of the facts if the documents of authority appear genuine, but the credit union must be able to verify the documents.

Finally, no matter how thorough the policies or well educated the employees are, there will always be an unusual situation that comes into a branch, probably more often than anyone would like. If there is ever any doubt on how to handle the account of a decedent, minor or other fiduciary, always consult with the credit union's attorney.

This body of law is vast and there are many nuances,but by implementing these steps, credit unions can offer the most protection possible to these most vulnerable members.

NCT

Wire Transfers

Jim Vilker
VP Professional Services
CU*Answers

Member Service & Teller

Believe it or not, over the past year there has been a number of wire-transfer fraud schemes that have cost our clients hundreds of thousands of dollars. Wire transfers are one of the easiest ways to steal from a financial institution, and you would be surprised at how the perpetrators get away with it. So why is it so easy? Most of the time it is either the result of social engineering or identity theft, and the ones that are really smart do a little of both. In one instance, the individual actually drove around neighborhoods detecting open Wi-Fi networks and uncovered an open non-password-protected PC. Once the criminal got into the network, he dropped a key-logging software onto the member's PC, which began recording all keystrokes and transmitting the information to the criminal. So what did he get? Everything about the member including home-banking logins, personal information that only the member would know, and the cell phone account sign-on and password. He then began to monitor the account on home banking and also began calling the credit union to gain the confidence of branch personnel. This went on for months. Unfortunately, the end result was a wire initiated by a phone call. Back-up procedures at the credit union dictated a call back and were followed appropriately. Guess who got called back? That's right; the criminal had also signed into the members cell phone account and had forwarded all calls to his own phone, so of course he was able to verify the wire amount and receiving party when the teller called. Sounds like something that could only happen in a big city, yet it happened in a small town in the Midwest.

As a credit union employee, wire transfers should be handled with the utmost attention to procedure, but also with good common sense. One thing I frequently see are wires being performed without the credit union ever asking the member why, even on non-domestic wires. Logical Reasons for performing wire transfers include having a child in active service overseas, having family members on a religiously-affiliated mission, businesses that frequently send their employees overseas, and students in foreign-exchange programs. Additionally, taking wire-transfer requests over the phone is problematic in itself. Validating a member over the phone, even if you do recognize their voice, as in the case mentioned above, is difficult without a substantial amount of out-of-wallet question sets. Most credit unions have discontinued this practice altogether without a signed authorization that was given to the credit union in person outlining all potential recipients. Taking a wire by fax or mail can also make it difficult to prove it was actually the member who initiated the request. I have heard of credit unions actually requiring a notary on such a request. Again, if the criminal is that smart, faking a notary would probably be in their arsenal of tools.

It's always best, even for the member, to second guess a wire transfer. It is in the best interest of the member that the wire is being done for valid reasons and being transmitted to a recipient who is deserving of the money. Almost every credit union has a story to tell about the member who is wiring money to buy a castle in the United Kingdom or who just needs to send $5,000 to pay the taxes on a lottery they have won in Nigeria or Jamaica. These are the tough ones. Those types of wires are being completed by the actual member who has been caught in a confidence game. So how does the credit union employee handle that type of wire request? The best thing to do is simply escalate those requests to senior management, who can then take the lead and counsel the member on the scheme of which they are a victim. Believe it or not, in many cases the confidence game has been played so well by the criminals that even after being counseled, the member continues with their plan to transfer the money.

From a back-office and auditing perspective, what does the back-office employee need to be cognizant of? Most importantly, they need to verify that the money being wired out is backed by good funds and that there are no recently-deposited checks that have not yet cleared. This is a very common practice and in some cases this requirement also falls on the individual who takes the wire-transfer request. Beyond that, the back-office employee should be reviewing the wire-transfer tracking log on CU*BASE. Recently, through the review of not only the CU*BASE log, but also the sampling logs of ACH items, a credit union uncovered a "money mule," which is a member who has been caught accepting funds from someone who obtained the money through internet scams. The scammer convinces the member that they will be receiving legitimate money and simply need to transfer the funds to another account,

continued on page 7

Word Search

C E N E D O R M A N T E R L T

R I S D N U F K S I R N L R S

E P A Y M E N T I U O A A E O

D C S M O N E Y S I W D M B P

I E E P W A T O T A E O P M R

T E O I D I L A R Z N U O E I

E T R E V C L D I I S A L M D

S E B I S U H R T S A M I R E

G I T I G T O O E R I O C C K

T C D E I H R N M N E G Y R O

A P R W T E I A O C A L M D V

O U S U H S N R H A A A L R E

O E A O U A D E P O S I T E R

E N L B G A C L L O R Y A P T

U D P E E K E F R A U D R R I

Word List:

REGULATION
TELLER
STOP
MONITOR
MEMBER
PAYROLL
MANAGE
DEPOSIT
POST
REVOKED
ACTIVITY
FUNDS
CHECK
MINOR
HOLD
DEBIT
PAYMENT
FRAUD
CREDIT
BUSINESS
POLICY
DISCLOSURE
UNAUTHORIZED
DORMANT
WITHDRAWAL
RISK
MONEY
WIRE

Wire Transfers

continued from page 6

which is almost always off shore. So what should the back office be concerned with? When performing a wire transfer, make sure you not only verify that the funds are good, but also where they came from. It is always a good idea to check if there has been a recent rash of ACH or incoming wire activity that the member is now channeling out to other accounts. If that is the case, dig deeper. Look to see where the funds originated. Call the member. In the case of the credit union that caught this, they simply asked the member to come in and explain what was going on. Remember, even though the funds that were coming into the account were actually settled, the origin was from illegal activity and because of that fact, the funds are not the property of the credit union or the member.

NCT

AuditLink

CU*ANSWERS Management Services

presents two exciting services
to assist with your auditing and compliance

PolicySwap

CU*ANSWERS

Trade policies with your peers.

Have a great policy?
Share it with the network.

Need a policy?
Download one from the network.

Sign up online at policyswap.cuanswers.com

All policies are reviewed by our AuditLink's staff of professionals.

ExamShare

CU*ANSWERS
A Credit Union Service Organization

Get prepared for your exam.

See what other credit unions in your area are experiencing with their audits.

Check out the hot topics for this exam period.

Share your experience with the network.

Sign up online at examshare.cuanswers.com