Issue 1 | November 2011

Network Compliance Teacher

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

In this Issue…

Editor's Corner

Welcome to the inaugural issue of the network compliance magazine. This magazine is designed for all credit union employees and was produced by compliance professionals using the GOLD system from across the country. The articles are written to give you some insight into how compliance related issues are addressed during your daily duties from other credit union perspectives. This is not your average boring compliance piece -- it's never the most exciting topic of discussion -- this magazine was actually written by your peers using the same system you use every day.

This quarter the group focused on a number of regulations including BSA, OFAC, and the US Patriot act. The authors each picked a specific area of the credit union including account opening, teller and loan, and back office. Our hope is that you will find a few tidbits in these articles that spark questions in your own credit union and maybe teach you a little something you were not aware of.

Jim Vilker, NCCO
VP of Professional Services
CU*Answers

Get Involved with the Network Compliance Teacher!

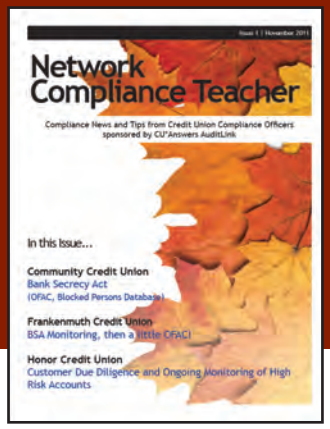
Have something to contribute?

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
Suite 100
Grand Rapids, MI 49525
(800) 327-3478
auditlink.cuanswers.com

Proud Member of the cuasterisk.com Network

Bank Secrecy Act (OFAC, Blocked Persons Database)

Terri Urbanek
Internal Financial and Operations Auditor
Community Credit Union

Internal Auditor

That pesky BSA Compliance Officer is at it again. Now they're asking how we know if the person for which we are taking a loan application has been cleared against the OFAC list! I thought only the tellers had to worry about that stuff? It's just a loan application, not a transaction. Did you know that CU*Answers can make life easier and ensure that none of your employees are working with a blocked or listed person? Auditors and examiners love it because the scan can be built directly into your controls.

The USA PATRIOT Act had a significant impact on the way financial institutions conduct business with the implementation of a Customer Identification Program (CIP) that requires a determination of whether the current or prospective customer appears on any list of known or suspected terrorists or terrorist organizations. The CU*BASE Data Match system provides a way to match your membership records against the current "Specially Designated Nationals & Blocked Persons" and the Palestinian Legislative Council (PLC) lists published by OFAC.

Process flow and Identifying Matches for OFAC and Blocked Persons

The process begins with the workflow controls for opening memberships. Workflow controls are used to organize day-to-day member service tasks. These controls provide enhanced compliance to your established account opening standards by managing the tasks an MSR must complete for a new membership or when taking a loan application for a non-member. On the workflow screen, if you have OFAC scan and check blocked persons file activated, the system will automatically run the applicant through these two processes after you enter their SSN/TIN and some basic information. If no suspected match is found, a window displaying this confirmation will appear. When you "Enter" to continue, the scan is recorded as a tracker conversation in the related member record.

Blocked Persons Database

The Blocked Persons Database can be used by each credit union to create a "Fraud Alert" list. This CU*BASE option allows you to record names and, if known, SSNs of individuals for whom membership should be denied. It can also be used to flag a particular name or SSN to indicate that additional verification of a person's identity may be required.

The scans begin with a look at the first and last name data fields. It will also compare text in the *City* field against any country names from the OFAC list. All accounts with the *Foreign Address* flag will be scanned against the country list. Organization names, not marked as individual, will be scanned against the first 30 characters of the name fields on the SDN list.

If the system finds an exact match of a name in both files, a warning will be displayed and staff should follow the credit union protocol for handling the data match. Because of the potential for a "false positive" where a name matches but other details such as the address do not, it is up to each credit union to review the items and make a determination as to whether it is a true match or not.

Disbursing Loan Funds

The loan is approved, the new member has cleared the OFAC and blocked persons check, and you are ready to disburse funds. Regulations require that you also verify payees against the OFAC lists. The February 2011 CU*BASE release introduced OFAC scans on payees of loan disbursement checks printed using MNLOAN #2 –Disburse Member Loan Funds, or if you disburse using phone operator, or an on demand OFAC scan of any item through the Timeout window, MNFILE #12 – Scan a Single Name Through OFAC, or via MNAUDT #4 – Scan a Single Name Through OFAC. Suspect hits where the birth date either matches the OFAC file or where the date is not in the standard format (MMDDYY) will show on the OFAC match report.

For more detail and monitoring procedures, please reference the guides below.

http://open.cuanswers.com/25m
http://open.cuanswers.com/25n

NCT

BSA Monitoring, then a little OFAC!

Jessica Hillborg
Compliance and Internal Audit
Frankenmuth Credit Union

Internal Auditor

BSA Activity should be monitored on a daily basis. This task is made much easier by the use of MNAUDT #1 – Work Daily BSA/ CTR Activity. The accounts that appear under this menu are set up by your credit union's own BSA configuration standards. The limits that you set will determine which transactions show up for you to monitor. This listing updates each day with the prior day's information. Each account should be verified individually. The key things that you are looking for here are:

- Does the transaction appear to have a lawful purpose?
- Is this type of transaction untypical or strange for the member?
- Does a CTR need to be filed due to the cash transaction being in excess of $10,000?
- Were multiple transactions done by the same member at different branches?

A majority of the accounts will be easy to verify. For example, perhaps a loan was disbursed and the member took the cash to pay for a vehicle or maybe the member cashed in a Certificate of Deposit. Transactions such as these are easy to review and move on to the next one. Sometimes, though, these questions may cause you to ask further questions of your staff to understand the intent of the transaction. If the BSA activity still seems strange after you have done some research, you may want to flag the account as higher risk and monitor the account for a certain period of time. The activity could even be suspicious enough for a SAR to be filed. The key to using this menu is to use the trackers that are created during the verification process. Make notes so if/when the account shows up again, you can more quickly determine how the member uses the account.

Another use for this menu is to verify that CTRs are being filed in a timely fashion. This menu can be used in conjunction with MNSERV #24 – Work with CTR Forms. If MNAUDT #1 shows that a CTR form needs to be filed on a member, then I can easily verify that the teller is filling out the form by verifying it exists in MNSERV #24. I can also spot check to make sure that the form is being filled out correctly and that the correct amount has been filled in.

MNAUDT #1 should be an integral part of your daily monitoring. If you make it a priority, you are sure to be on top of possible BSA violations in regards to member transactions!

The next item under MNAUDT that should get a decent amount of attention is #3 – Run OFAC Data Match. How often you run this scan will depend upon your credit union's procedures. I have spoken with many credit unions that run it on a bi-weekly basis. This is fine to do, just make sure that you document how often you will run it and then follow through. The scan is simple to complete, CU*BASE does most of the work for you by flooding in the information on the OFAC and PLC lists, as well as the list of sanctioned countries. You can narrow down the dates that you want the scan to be run against, but I typically leave the dates blank and scan the entire membership.

Once a list is generated with matches, it is critical to dig deeper to determine whether matches are positive or false-positive. This can be done by going to the actual OFAC list on the U.S. Treasury's website (http://open.cuanswers.com/25o) and searching for the name that shows up as a positive match. From here, you will be able to gather more information, such as address, date of birth or social security number that can be used to compare against your member (or non-member) to determine if it is a true match. If it is not a true match, document and retain that documentation for when the name appears again on future scans. If you do have a true match, follow your procedures and contact OFAC immediately at their toll-free hotline: 1-800-540-6322. The OFAC resource center (via the link above) contains a wealth of information that may be able to answer any other match-related questions you may have.

NCT

MSR/Account Opening – CIP Red Flags

Amanda Craig
Compliance Officer
Honor Credit Union

Member Service

The USA Patriot Act requires credit unions to implement procedures that at a minimum verify the identity of any person seeking to open an account, and to maintain records of the information used to verify a person's identity. Most credit unions provide the required notice to members and potential members describing the customer identification process as signage in new account offices. But how do you verify the accuracy of an applicant's information? CU*BASE workflows can be configured to automatically provide the tools necessary. The first stop in validating information and spotting red flags (discrepancies) is reviewing the identification presented. It may sound elementary, but do you always compare the appearance of the person presenting the identification with the picture ID when opening a new account or adding a joint owner? Do you review the documents for alterations or forgery? Make it a habit to take a few seconds and do this.

The next investigation tool is the Credit Report. Do the name and SSN entered into CU*BASE match what's reported? (Helpful Tip for Equifax: The first name and SSN to appear on the Credit Report are how information was entered into CU*BASE. The second name and SSN are what the credit bureaus are reporting for that individual.) Also, review the current and previous addresses—some credit unions require previous address information if an individual has lived at an address less than two year. Former names are useful in identifying aliases and don't forget to review the fraud summary to see if there is a fraud victim indicator.

CU*Answers also offers Experian's AS1 which authenticates the member's name, address, SSN, date of birth, Driver's License Number and Phone Number against Experian's File One credit database of more than 200 million credit-active customers. This is an excellent service for the credit unions using it as it gives results of pass, partial pass, and fail, including detailed results of why an identifier failed or passed.

How do you reconcile any differences? First ask the member for clarification, explanation or further details. The member should be able to clearly answer your questions. Listen to their response carefully. Trackers are an excellent, permanent record of your due diligence efforts in response to red flags. Trackers should be unbiased and balanced accounts stating facts, statements made by the member and your findings. Remember trackers can be reviewed by anyone in your organization or examiners and may be used in legal matters.

Be familiar with your Customer Identification Policy (CIP). What types of identification does your credit union accept? Does your policy allow for non-documentary verification methods, and if so, who may perform those? What are your credit union's procedures in the event of lack of verification? Are you prepared to tell a potential member you are unable to open their account because you cannot form a reasonable belief regarding the true identity of the person? Review with your BSA Officer how to handle these situations so you aren't caught off guard.

NCT

Teller Red Flags

Amanda Craig
Compliance Officer
Honor Credit Union

Teller

CU*BASE records changes made to a member's name, email, phone and address for 30 days. A Red Flag warning message will appear each time the account is accessed, containing the number of times contact information has changed. Audit trackers show: who changed the information, what was changed, and when the change was made. Reviewing the audit tracker is a great place to start if you have a funny feeling. Determining why the records were changed and if they make sense is the next step in fighting identity theft. Ask the member during the transaction, "Did you recently change your contact information?" It could be something as simple as the member enrolled in e-Statements and their email address was obtained. Or you could uncover potential fraud on the account. Each credit union has Red Flag policies and procedures in place to prevent contact information from being changed by someone other than the account owner, but your help in fighting identity theft is critical. As front line staff, your direct contact with the member provides a unique opportunity to dig deeper by asking questions. So next time the warning message pops up, don't pass by it quickly, think if how many times contact information has changed makes sense and review changes with the member if necessary.

NCT

Teller OFAC Scans

Amanda Craig
Compliance Officer
Honor Credit Union

Teller

Tellers have the convenience of CU*BASE automatically performing an OFAC scan on the payee of outgoing wires, upon creation of corporate checks or money order for the payee , and when an A2A relationship is created. Some transactions require tellers to manually complete an OFAC scan using the on demand OFAC scan (available from F18 in the time out menu) such as a Power of Attorney performing a transaction and who is not listed on the account. The U.S. Department of Treasury instructs "Every transaction that a US financial institution engages in is subject to OFAC regulations," so when in doubt it is a best practice to manually perform the scan. Don't forget when performing a scan to switch between an individual or organization name to get an accurate result.

Automatic scans are written out as an audit record on the member's account to serve as verification that an OFAC scan was performed. Manual scans are also recorded and accessible by your BSA Officer to serve as documentation. But how does your credit union handle possible matches? Hits should be verified against the *OFAC Specially Designated Nationals (SDN) and Blocked Persons List* (http://open.cuanswers.com/28l). The Treasury provides guidance on evaluating the quality of a hit on their website (http://open.cuanswers.com/28m). But how do you document all the due diligence you've performed on the legitimacy of the hit? One possibility is to update the audit tracker using memo type "OFAC/PLC Overrd" including details on what steps were taken and the results of the investigation. As front line staff you must adhere to the requirement to not violate the law by doing business with a target, so never provide services to a person named on the SDN list and get your BSA Officer involved if you require assistance.

NCT

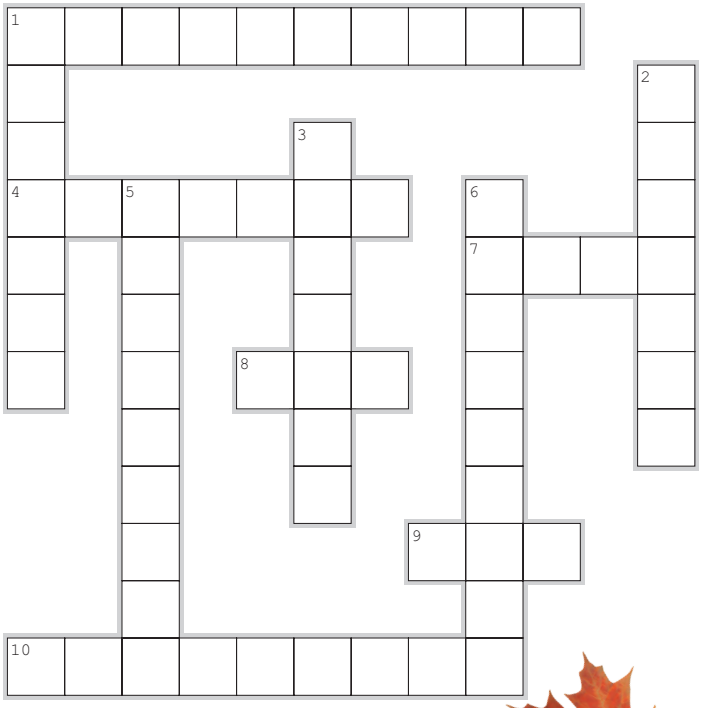
NCT Crossword

Across

1. SAR stand for _____ Activity Report
4. When a member changes their address it is considered a _____
7. Office of Foreign Asset Control (acronym)
8. Your _____ determines how you properly identify the individual opening an account
9. Acronym which stand for Personal Internet Branch
10. The SDN list stands for _____ Designated Nationals

Down

1. Bank _____ Act
2. _____ Persons Data Base is a feature of CU*BASE to list names of people who have tried to defraud the credit union
3. The USA _____ Act requires that you verify the identity of any person seeking to open an account
5. The member due _____ flag allows you to track high risk members on the CU*BASE system
6. Terri Urbanek works at this credit union



EclipseCrossword.com

Customer Due Diligence and High Risk Accounts

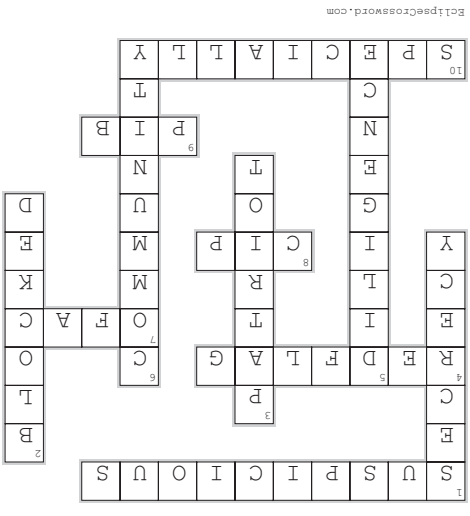
Joe Spenski
Audit Link Associate
CU*Answers

Implementing a comprehensive Customer Due Diligence (CDD) program is a key pillar of a strong BSA compliance program. The objective of CDD is to enable your credit union to predict with relative certainty the types of transactions that a member is likely to engage in by verifying a member's identity, occupation, etc. Once you have the proper policies and procedures in place to determine potential high risk members, CU*BASE will help with your due diligence processes. CU*BASE allows you to code any member with a due diligence flag (1-9) and then monitor the member in a weekly, bi-weekly, or monthly set of transaction and maintenance reports. These transactional reports can be pulled from MNAUDT #17 – Insider Audit/ Due Diligence Rpt. The flag can be placed on the member's account during account opening when you gather your initial information, or at a later date when you learn of high risk activity on the member's account. CU*BASE does not have an option to configure the meanings of your DD flags, so you will need to keep a separate spreadsheet for that.

How do you find high risk transactions?
CU*BASE recently added two new menu options to the Audit Menu. MNAUDT #9 - Sample High-Risk Checking Accts will gather all of the transactions that occurred on the only the checking accounts and MNAUDT #10 – Sample High-Risk Transactions will gather all of the transactions for all of the suffixes. Both of these report options will break down all transaction activity by thirteen different analysis methods. Audit Link recommends that at the beginning of each month, the credit union spends time reviewing the top ten accounts in each analysis method. By doing this you will gain an understanding of what "normal" activity is for each area, while uncovering members that are processing business transactions through their personal accounts by means of ACH, check kiting fraud, or the profit or loss for each member (to name a few).

Once you code these members with a due diligence flag, you will need to establish a timeframe to pull the Insider Audit/Due Diligence Report from MNAUDT #17. One item to consider when deciding on your timeframe is that weekly or bi-weekly reviews—as opposed to monthly—will make the process more manageable as you will have less information to sift through each time. Note that should you get to fifteen or more members, there are a lot of transactions to review.

NCT



Using Personal Internet Branch at Account Opening

Patrick Sickels
Internal Auditor
CU*Answers

Online Services

From a regulatory standpoint, starting in 2011 the NCUA will be examining credit unions to determine whether layered security has been applied to high risk online accounts. According to the 2010 FFIEC Guidelines for Internet Authentication, high risk online accounts remain defined as "electronic transactions involving access to customer information or the movement of funds to other parties." So when a member wishes to open an account that includes online banking, the first question a credit union should ask is whether this account will be defined as high risk. If the member is looking to transfer funds using A2A or use online bill pay, that online account automatically becomes high-risk. Fortunately, CU*BASE provides a layered security system called Personal Internet Branch, or PIB, that can immediately reduce the risk of online banking to both the member and the credit union. The easiest time to address the risk is at account opening.

Reduce Risk with PIB

PIB offers a multitude of ways to reduce the risk of online banking. First of all, transfers and other transactions can be limited to a maximum daily or monthly amount. Certain types of transactions can also be configured to ask for a confirmation code. You can limit transactions by days of the week, time of day, and even the PC's that can access online banking. Your member can also get an email confirming when a transaction has taken place.

Certainly, a credit union that has a high risk online account should at minimum require that the member get an email confirmation of all transactions, and consider having a confirmation code for high dollar value transactions. Consumer protection need not be scary either; even if you are a small local credit union, you have a state of the art security platform in PIB. While you provide the service your members expect, PIB is working in the background as a state of the art system protecting your members.

At account opening, credit union staff members can helpfully suggest that PIB is an excellent way to protect the member as well as the credit union. None of this should discourage a member from having an online banking account; instead these are enhancements to the security of the member's money. Setting up PIB can be done in a short period of time and goes a long way to protect your members and you. Emphasizing that PIB is a normal part of online banking will also go a long way to ensuring the confidence of your members. PIB is a way to build member loyalty by demonstrating the commitment your institution has to the protection of the membership.

More information on PIB can be found at:
http://open.cuanswers.com/25k
http://open.cuanswers.com/25l

NCT

Coming in 2012

AuditLink

CU*ANSWERS Management Services

presents two exciting new 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.

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.

Details coming first quarter 2012