Case Studies
HANDOUT

BSA Graduate School

January 2018

Table of Contents

Case Study #1 – Due Diligence and Willful Violations

A six-branch community bank in West Virginia received a civil money penalty of $4.5 for willfully violating the Bank Secrecy Act. The bank had severe and systemic failures in many aspects of its anti-money laundering program. Because of these failures, the bank processed millions of dollars in structured and other suspicious cash transactions.

Failures

- The bank failed to identify high-risk customers. Consequently, high-risk customers were not effectively monitored for suspicious activities.
- The bank failed to file more than 400 Currency Transaction Reports (CTRs) in relation to this customer alone. During the examination, the bank's regulatory agency found a total of 619 CTRs that were not filed.
- The bank failed to file Suspicious Activity Reports (SARs) on obviously structured transactions.
- Failure to adequately staff the BSA department
- Failure in establishing dual controls
- Failure to have an effective independent review/audit
- When questioned about the activity, the Branch Manager lied to the FBI and IRS.

How the Scheme Worked

The corporate customer, a company that supplied labor to mining companies, paid its employees in cash to avoid paying employment taxes. A vice president/branch manager of the bank advised the employment company to request draws on a line of credit and have employees of the company pick up the funds, issued in cashier's checks. The cashier's checks were cashed at the bank, but could also be cashed at another non-related financial institution.

In addition to paying mining employees in cash, the company also paid kickbacks and bribes in cash to others. The transactions appeared on daily cash reports, but the BSA Officer failed to identify the structured transactions as suspicious. The transactions should have been aggregated and CTRs should have been filed, which the BSA Officer also failed to do.

Additional Issues

The Bank had invested in AML software but failed to utilize it. When questioned, employees of the affected branch admitted to being aware of the activity but were too intimidated by the manager to report it. In addition, the BSA Officer was related to the manager, so employees did not know what recourse they had.

Initially, it was felt that the BSA Officer was overworked, understaffed, and had not received enough BSA training to effectively oversee the BSA program. As additional facts came to light, it was the opinion that the BSA Officer purposely ignored CTR and SAR filings and has since been banned from banking entirely. Though he faced five years in prison and a $250,000 fine, the Branch Manager received only 3 years' probation and a $5,000 fine. He also has been banned from banking.

Changes

The Bank has hired a new BSA Officer and the department is adequately staffed with effective dual controls. The AML software is now fully functional. Changes were made in who conducts the independent review/audit. The consent order has been lifted.

Case Study #2 – Due Diligence and Knowing Your Customer

A community bank in North Carolina paid $400,000 towards restitution to victims of a Ponzi scheme that operated through accounts maintained by the bank.

A customer of the bank laundered more than $35 million through his accounts over two and a half years. The customer used an account with the bank to hold and disperse funds. The bank failed to detect suspicious activities that consisted of large cash withdrawal transactions, ACH and wire transfers, and gift card purchases. The customer purchased private jets, high-end vehicles, and other expensive gifts. The customer was also investing in the foreign exchange market.

Noted Issues

The Bank failed to "know your customer," as admitted by the Bank's CEO. The Bank's AML program was deficient. The Bank's customer due diligence and enhanced due diligence monitoring was deficient.

No bank employees were found to be complicit in the Ponzi scheme. The Bank is currently being sued by nearly three dozen victims who had invested with the bank's customer who claim the bank was at fault for turning a blind eye to suspect activity.

Case Study #3 –Due Diligence with CIP and Foreign Customers

An Indiana community bank spent months preparing a three-weekend event geared to reaching out to its large, unbanked, Hispanic community. The decision was made that the only identification requirement would be provision of a cedular or matricula consular card. If a person has a cedular card, they should also have a passport, passports were not required. A person with a matricula card may not have any other form of identification.

The drive was a success; hundreds of new accounts were opened. Shortly after, two of the new customers were arrested for operating a counterfeit identification ring.

What are the ramifications and what could have been done differently?

Case Study #4 – Due Diligence with Dual Controls and Employee Account Monitoring

A wealthy, elderly customer of a community bank made an appointment with his accountant. The accountant, who routinely pulled an annual credit report for his customer, questioned the gentleman on loans made with a particular community bank. The perplexed gentleman stated that although he had time deposit accounts with the bank, he had not borrowed any money. He stated that he would get to the bottom of the issue.

Upon visiting his local branch, he approached the manager with the facts provided by the accountant. The branch manager, who happened to be the BSA Officer, was a smooth talker who eased the gentleman's concerns by supposedly reviewing the customer's banking history on the computer and stating no loans had been made, there must be a mistake, and whatever it was, she would take care of it - he had nothing to worry about.

The gentleman reported back to his skeptical accountant who detected something amiss. The accountant contacted the bank president and a discreet investigation began. It appeared that the BSA Officer, who had been hired just 18 months prior, had been writing loans in the gentleman's name, using his CDs as collateral. She had opened an account in the name of her mother, who had Alzheimer's, and funneled the proceeds to herself through the mother's account. The investigation also found the elderly gentleman was not the only victim; she had also written bogus loans in the names of other customers, keeping the funds for herself. She had also conducted illegal withdrawals totaling more than $33,000 from her mother-in-law's account. The combined theft totaled more than $159,000.

The BSA Officer was sentenced to two years in prison and was ordered to make restitution.

Case Study #5 – Due Diligence with Privately Owned ATMs

A Rhode Island bank entered into an agreement with a cash-dispensing systems company (The Company) whereby The Company would place automated teller machines (ATMs) in convenience stores, gas stations, and other businesses and the machines would display the Rhode Island bank logo. Even though the machine carried the bank's logo, The Company was responsible for setting up the machines and contracting with merchants. The Company would also be responsible for ATM maintenance.

The Bank would be responsible for providing cash for specified ATMs. The Company would be responsible for some, while merchants supplied cash for other machines. Over time, the number of ATMs in the network that were funded by the bank increased while the number of ATMs funded by The Company decreased.

Personnel at The Company devised a plan whereby excess cash would be ordered from the bank and would be used to fill machines normally filled by The Company. The employees of The Company also engaged in a cover-up to try and prevent the bank from recognizing that money was missing by "floating" the bank's money. That meant, the extra money ordered was also used to fill ATMs that had been shorted cash. This continued for a few years, resulting in a loss of $4.8 million to the bank.

What Went Wrong

Bank BSA staff never conducted any due diligence, never monitored, and never requested receipts to balance actual funds dispensed with cash orders. Information provided by The Company was never questioned or verified.

The bank has since been sold.

Case Study #6 – Due Diligence at Account Opening

During an independent review, it was recommended that a community bank implement procedures at account opening that would allow it to formulate a profile of a new customer, thereby identifying customers that may warrant monitoring from the beginning of the relationship. One of the questions asked was whether the customer would have a need to conduct wire transfers. In this instance, the customer, a young woman, stated yes, one transfer per month would be conducted to her boyfriend who was in the military.

Since the wire transfer question elevated the customer's risk rating, the BSA Officer monitored the activity. After a month of monitoring, the BSA Officer contacted the consultant to ask if it would be acceptable to close the customer's account for not using it in a manner consistent with stated use at account opening. The customer had conducted seventeen (17) transfers during the month and none to the same person.

The consultant said yes, it would be permissible and that the information would be reviewed since the consultant would be coming to the bank on the next business day.

Upon review of the transactions, the consultant questioned the source of funds, which were ACH transfers held in an account at a bank in Alabama. The information was not known since the customer was local and known to some bank employees as she had worked at a local business for some years. Upon speculation and experience with unusual activities across the country, the consultant suggested the woman was involved in some online scheme/scam. That same day, another ACH transfer was deposited to the woman's account and she called the bank to state she would be in to conduct a wire transfer in the afternoon, as she had not yet received the letter stating her account would soon be closed.

Soon after, the BSA Officer stated that she had received a call from the bank in Alabama. They wanted to know why this bank's customer was transferring money from their Habitat for Humanity account. It seemed that Habitat had just received their monthly bank statement and discovered the transactions during balancing.

The remaining funds in the community bank account were frozen and the local police were contacted. When the customer came to the bank, she was sequestered in an office and questioned by bank staff and local police. She was the unwitting pawn in an online romance and the wire transfers were supposedly going to servicemen who didn't have bank accounts so their pay would be sent to her "boyfriend's" account at the Alabama bank and she would forward it to them when she received the ACH transfer where it was to be picked up at the base where they were stationed. The month's total was over $27,000.

Case Study #7 – Let's Talk About It

The owner of a bank's exempt Phase II business comes to your bank to purchase a cashier's check on behalf of the business. The check is paid for with cash and is in an amount that would normally be CTR reportable.

How would you handle it? What issues are present?

Case Study #8 – Let's Talk About It

Your bank, which is registered for sharing information with other financial institutions under Section 314(b) of the USA PATRIOT Act, receives a request to share information. It appears the information being requested applies to a customer that is kiting, which you have already identified.

Explain how you will handle this.

Case Study #9 – Let's Talk About It Some More

Your bank, which is registered for sharing information with other financial institutions under Section 314(b) of the USA PATRIOT Act, receives a request to share information. The requesting institution sends not only an email but also calls and leaves a voice message requesting that you expedite the request.

You email the requesting institution and ask for verification from their 314(b) contact since the person requesting the information is not listed as the contact. You receive a compliant email from the designated contact. The story provided by the fraud specialist, who initially emailed you, states their customer has been caught up in a lottery scam and almost $10,000 has been transferred to an account at your bank.

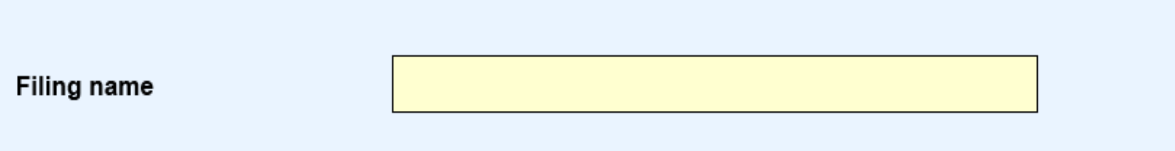
The information being requested is:

- To whom the account held at your bank is registered,
- When it was opened and by whom,
- The names of authorized signers,
- The nature and purpose of the account,
- The source of account funding, and how have the funds received from the requestor's bank have been used.
- If the funds were dispersed, the dates, amounts, and payee names, along with method of payment.
- They also want to know if your bank has had any concerns related to the customer that are relevant to the requesting bank.

Your initial response to the bank is hesitant. What would you consider and what would be your response?

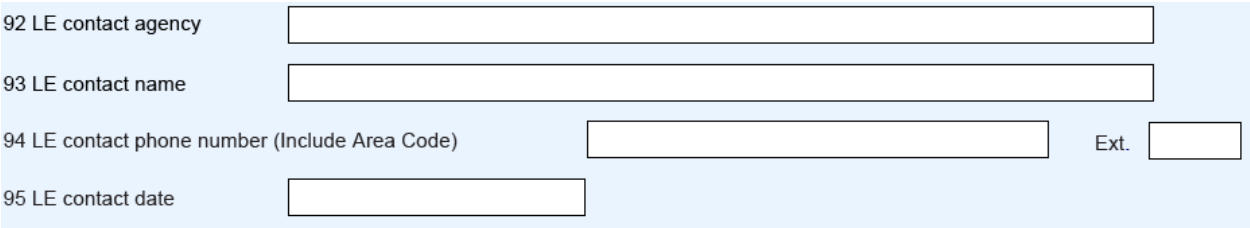
Suspicious Activity Report (SAR) Filing name

FinCEN strongly recommends that financial institutions not use the name of the subject (suspect) in the filing name. They state that a method of naming SARs should be used that allows a bank to easily track SARs for recordkeeping and audit/exam purposes without including the suspects name.



Part IV – field 92 – LE Contact agency

If you have contacted law enforcement (LE), enter the agency information here, include the name of the LE contact in field 93, the telephone number of the LE in field 94, and the date of contact in field 95.



Part III – fields 51 – 60

Common error in transferring all information from Part IV over to this section. If you notice, the heading states "Part III Information about Financial Intuition Where Activity Occurred

If some or all of the activity occurred at the main office listed in Part IV, then it would be appropriate to list it in this section. **If none of the activity occurred at the main office listed in Part IV**, the information should not be carried over.

In FinCEN SAR FAQ's, number 19, it states:

> **You would include the RSSD number associated with the "Filing Institution" in Item 84 (Part IV) and that of the "Financial Institution Where Activity Occurred" in Item 51, which could be a branch location. When the activity being reported occurs at additional branch locations, you should include the RSSD number associated with the additional branch(s) in Item 66.**

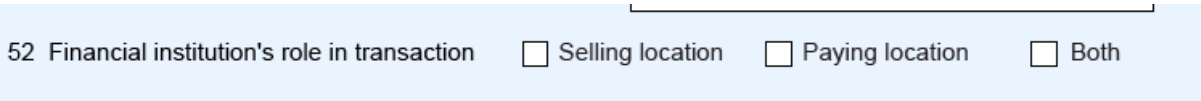
If you have a branch that has not yet been assigned an RSSD number, leave the RSSD number field blank. (Paragraph 2, question 19.)

FAQ #20, paragraph b. clarifies further by stating:

b. A single depository institution with multiple branches files their SARs out of the home office of the depository institution. In this scenario, Part IV would be completed with the information of the home office of the depository institution, and then a Part III would be completed for the depository institution location where the activity occurred. If the activity occurred at additional branch locations of the depository institution, then that information would be entered in Items 64 – 70, and would be repeated as many times as necessary. In Part IV, the filing institution should enter the name of the contact office that should be contacted to obtain additional information about the report.

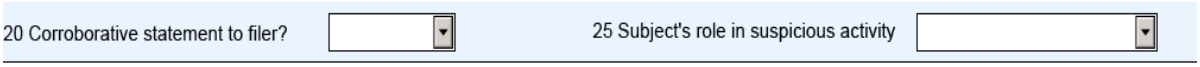
If the activity took place at a **single branch** (not main office listed in Part IV), you will check the box at the bottom of the SAR that states:

Part III, field 52 –



Refer to Part II, fields 39 and 40. If the suspect purchased any of the instruments recorded in this section from your financial institution, you would check "selling location." If the suspect received payment from any of the instruments recorded in fields 39 and 40, check "Paying location." If instruments listed in 39 and 40 were **purchased and cashed** at your financial institution by the subjects listed in Part I, check "both."

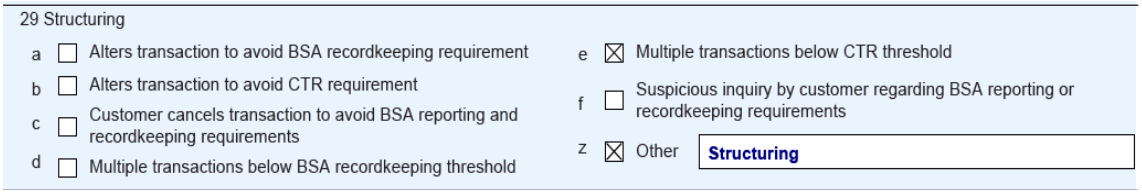
Part I, field 20 is routinely found to be incomplete



For example, if your customer asked an employee how much could be transacted before a "government report" would have to be filed or mentioned they did not want a government report filed, and proceeded to structure the transaction, they have technically acknowledged that they understood what they are doing. In that case, the box would be completed with "yes." If nothing was said, then complete with "no." This field should always be completed with something.

Field 25 – again, we will look at fields 39 and 40. If the subject's role in the suspicious activity was to purchase or send the financial instruments (or products) listed in 39 or 40, you will select "purchaser/sender." If the subject was the payee or receiver of instruments or products listed in 39 or 40, you will select "payee/receiver." If they were both, then select "both."

Use of the "z" Other field in any part of Section II. FinCEN noted in their SAR Activity Review that financial institutions routinely use this field incorrectly. For example, within Part II, field 29 structuring, may be (incorrectly) completed as follows:



FinCEN requests that "z" Other be completed only to further clarify the characterization that is listed or use it when no other characterizations listed adequately describes the suspicious activity.

Part V – Narrative Issues

- If amending a previously filed report – **Do** begin the narrative by describing how the report is being amended. Also, refer to the Document Control Number (DCN) if available and the date of original filing.
- If filing a SAR for continuing activity – **Do** begin the narrative by stating it is a follow-up SAR, refer to the previous DCN (if available) and the date of last filing. **Do not** copy and paste narratives from previous SARs into the follow-up SAR.
- If a suspect is listed in Part I, it is not necessary to list their name and identifying information again in the narrative.
- **Do not** list a victim of a scam as a suspect in Part I. You may include complete victim information in the narrative, but FinCEN specifically states do not list them as a suspect.
- **Do** list specific dates and dollar amounts when describing the period of time the activity occurred. For example, if you say, "the customer structured transactions in the amount of $60,000," FinCEN cannot determine if the transactions were truly structured. If you state the customer "deposited $10,000 in currency on May 8, $10,000 on May 10, $10,000 on May 11, $10,000 on May 15, $10,000 on May 16, and $10,000 on May 18" it is easier to evaluate the information being reported.
- **Do** state how the activity came to your attention. If your institution utilizes an employee SAR referral form, and the activity was reported in this way to the BSA Officer, state that. If your AML software generated an alert, state that.
- **Do not** include details that do not relate to the suspicious activity.
- **Do** complete Part I, when known, on individuals who use a business to conduct suspicious activities. Too often, Part I is completed in the name of a business, but it was the owner/manager/employee who conducted the activity through the business.
- **Do** explain (if not obvious) why you find the reported activity suspicious. "These transactions are suspicious since they are outside the historical norm for this customer," for example.
- **Do** feel free to describe the supporting documentation that is maintained if not included in any approved format attachment.
- **Do** include dates of transfers, originating or receiving account numbers and of other affected financial institutions, when appropriate. You may be providing a completed puzzle or providing a piece to a puzzle that is in progress.

Keep in mind that you are trying to convey to a stranger who has no knowledge of a situation, why this activity was worthy of notice and reporting. You are telling a story without writing a thesis.

Privately Owned ATMs

According to the 2014 BSA Exam Manual, "Privately owned ATMs are particularly susceptible to money laundering and fraud."

A privately owned ATM may be owned, leased, and/or operated by the merchant in whose establishment it is located. It may be owned and operated by another financial institution, or it may be owned and operated by an independent sales organization (ISO) who pays the merchant a set amount of money or a percentage of fee income to allow placement of the ATM in their shop. Please refer to the BSA exam manual for more information on ISO's and how they operate. We will be focusing on risk and mitigating that risk.

Identifying Risk

One problem is many states do not require registration of, limit ownership, monitor, or examine privately owned ATMs or their ISOs. A provider of an ATM or the merchant that houses the ATM may be unaware that the ISO, which operates the network, has changed ownership or has subcontracted management to another company.

Again, according to the BSA Exam Manual, money laundering can occur when an ATM is replenished with illicit currency that is then withdrawn by legitimate customers. This allows all three phases of money laundering to take place, (placement, layering, and integration).

We have provided guidance, based on a client's risk, on management of this area. The first step would be to address privately owned ATMs in your bank's policy, procedures, and BSA/AML risk assessment.

The next step, which many banks have not yet taken, is to identify current customers that own/operate a privately owned ATM. Typically, you will find the machines in grocery stores, gas and convenience stores, liquor stores, bars, and restaurants.

Another step is to identify, at account opening, new customers who have an ATM on their premises and determine the relationship and risk represented. It is much easier to manage and implement enhanced due diligence when you identify the risk at the onset of the relationship.

At Account Opening

- Document corporate licenses, operating permits, and contracts
- Document currency-servicing arrangements, including the source of replenishment of currency.
    - Review lending agreements, armored car contracts, or other documentation
- Verify who will conduct maintenance and balancing of machine(s)
- Verify the length of time the customer has maintained/operated the privately owned ATM
- Review public databases for public-cited problems, lawsuits, or concerns related to the ISO or principal owners.
- Document the location of each privately owned ATM
- Identify the target geographic market

- Document expected monthly dollar amounts of currency withdrawals
- Document expected monthly volume of transactions
- Verify what transactions can be conducted through the ATM
  - If it's an ATM owned/operated by a financial institution, a wide range of services may be available
- Verify who maintains insurance covered against theft and damage

Ongoing Due Diligence

Ensure you have up-to-date knowledge of the number of privately owned ATMs owned/operated by your customers. Ensure that your policies and BSA/AML risk assessment address the risk and due diligence that will be in place.

Based on your identified risk, ongoing monitoring procedures should consider the following, *as applicable:*

- Ongoing verification of the number and location of privately owned ATMs
- Any changes to the physical location/address of the machines
- Any changes to the targeted market area
- Compare expected monthly dollar amount levels with actual transaction dollar amounts
- Compare the number of expected monthly transactions with the actual number of monthly transactions
- Compare withdrawals of currency from your institution for the purpose of replenishment of machines to withdrawal receipt totals
- Review account statements for settlement processing
- Verify who is conducting maintenance on and processing transactions
- If the merchant replenishes machines from own funds, there should be a corresponding drop in cash deposits.
- Verify that theft/damage insurance continues to be maintained
- Review lending agreements between the business and the bank or other currency provider
- Review that permits are current and valid

Multiple Transactions Case Study

Multiple transactions take place for ABC grocery store. Two cash deposits totaling $7,800 are received through the night drop and one cash deposit of $6,500 is received through the teller line, delivered by Employee A of the grocery store, who was identified by frontline staff.

Part I, line 2, box (c) *Person on whose behalf transaction was conducted will be checked.*

Part I, field 3, "Multiple transactions" box, should be checked and Part I completed in its entirety for ABC grocery store. The affected account number and total cash in of $14,300 will be listed in field 21.

An additional Part I should be completed for Employee A, who made the deposit of $6,500.00. "Multiple transactions" *will not be checked* in Employee A's Part I. $6,500.00 and the affected account number should be listed in field 21.

In Part II, check the "night deposit" box in line 24.

From a hotline submission, what would be the correct way to handle this scenario?

Company A

The business is an LLC and Mr. Gray is 100% owner

Mr. Gray is listed as the registered agent on the state website

Mr. and Mrs. Gray, husband and wife, are signers on the account

Mr. Gray, along with employees 1 and 2, regularly deposit reportable amounts of cash to the business account and CTRs are filed throughout the week.

Company B

This business is an LLC with Mr. Yellow and Mr. Red as managing members

Mr. Gray is the registered agent on the state website

Mr. Yellow and Mr. Red are signers on the account

Mr. Yellow conducts the majority of transactions, but occasionally Mr. Red and employee 1 (from Company A) will conduct deposits

Alone, Company B does not conduct cash transactions in amounts that require a CTR. Because the banks BSA software is tying Mr. Gray to both accounts, the software is aggregating transactions and stating that Company B should be included on the CTR.

Aggregate and report or not?

Currency Transaction Report (CTR) Clarifications

Part I, Occupation/Line of Business

Across the board, we note ongoing issues with the occupation/line of business and NAICS code fields. In conversations with FinCEN, FinCEN has stated that there is an expectation that Part I, field 9, *occupation/line of business* will consistently be completed with a detailed description. The NAICS code field (9a) expectations for completion apply only if there is an *exact or very close match*. If not, it may be left blank. Review of examination recommendations consistently note financial institution employees using generic terms in field 9. Additionally, if Mr. Blue works for the gas/convenience store, his occupation should not be listed as "gas/convenience store" but should list, for example, "gas station clerk" or "gas station owner." Nit picking? Comments from actual examinations.

Part II, Transaction Details

We consistently find financial institutions listing "ON-US" cashed checks as "Withdrawals" in Part II, field 27. There seems to be some confusion in thinking that Item (d*) Negotiable Instruments Cashed* is only selected when a foreign check is cashed. If it is a withdrawal or debit from an account, line (a) Withdrawals should be completed. For any withdrawal by a negotiable instrument, select line (d) *Negotiable Instruments Cashed*.

Part II, Aggregated Transactions

In order to use this field, three factors must exist:

1. None of the multiple transactions being aggregated can be greater than $10,000
2. No one conducting any of the multiple transactions was identified (because all transactions were less than $10,000.01)
3. At least one transaction must have taken place through the teller line

On February 20, 2016, FinCEN announced changes and updates to the CTR. Single filing financial institutions were required to begin using the new CTR in August 2017 while batch filers had a reprieve while technology caught up with the changes.

Changes

Part I, item d was changed from "Courier Service (private)" to "Common Carrier." If a customer contracts with a third party to conduct reportable transactions, this field would be selected. Additionally, they referred to FIN-2013-R001 to clarify that the individual driver of an armored car service (ACS) would not be required to provide identification, but Part I would be completed for the ACS company providing the service for the customer, as well as for the business on whose behalf the ACS was working.

In Part II, the field "Shared branching" was added to line 24 for transactions conducted by or on behalf of another financial institution that is a member of a co-operative network (applied to co-op credit unions.)

Part III

- Added an Unknown option to Item 29, Primary Federal Regulator
- Added an Unknown checkbox to Item 32, EIN
- Added Item 37, Country
- Added Item 41, Cash in amount for transaction location
- Added Item 42, Cash out amount for transaction location

Part IV

Part IV, "Filing Institution Contact Information" was added to collect data about the institution filing the CTR.