

Best Practice Recommendations Suspicious Activity Monitor

ACH Monitoring Feature

Revised July 9, 2019

Disclaimer of Liability

Disclaimer of liability: We're often asked for Best Practices in using our software. Unfortunately when it comes to detecting money laundering, fraud, identity theft, financial abuse of the elderly and other nefarious activity, there isn't one strategy that works for all financial institutions. However, based on our years of experience, we do offer the following recommendations as a starting point.

Very important note: Please understand that the procedures we recommend in this document may be different from what we recommended in previous documents. We update our Best Practice Guides periodically, to reflect what is current in the banking and credit union industries. The bad guys are always doing new things—and these guides help you stay one step ahead!

This copyrighted document is owned by Wayne Barnett Software (WBS), a Texas Corporation. It is intended solely for the use of WBS current and prospective customers. Any distribution of this copyrighted document by anyone other than Wayne Barnett Software is prohibited, unless written permission is first received.

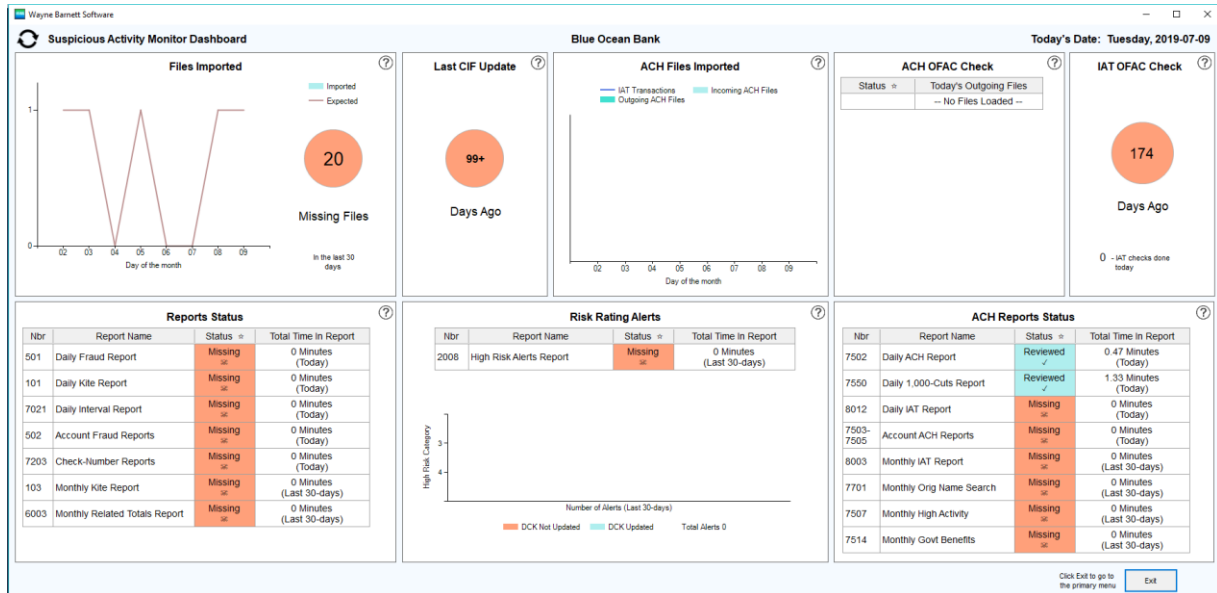
Table of Contents

Contents

SAM Dashboard	1
Daily Best Practice 1: Import all ACH files (both incoming and outgoing) into SAM	2
Daily Best Practice 2: Analyze outgoing files for fraud	4
Daily Best Practice 3: Analyze incoming files for fraud.....	13
Daily Best Practice 4: Search for Pink Cowboy Boots Fraud	20
Daily Best Practice 5: Search for 1,000-Cuts Fraud-.....	24
Daily Best Practice 6: Check IATs for OFAC Compliance	27
Daily Best Practice 6: Review IATs for Suspicious Activity	29
Bi-Weekly Best Practice 1: Update the CIF	31
Monthly Best Practice 1: Monthly IAT Review	33
Monthly Best Practice 2: Monthly ACH Originator Review	35
Monthly Best Practice 3: Monthly ACH Trigger Review.....	38
Monthly Best Practice 4: Monthly Alert Report Review	46
Monthly Best Practice 5: Monthly Review of Government Benefit Payments.....	49
Monthly Best Practice 6: Monthly Review for Crypto Currency Transactions	51
Quarterly Best Practice 1: Risk Rating Cleanup	53

Dashboard

SAM Dashboard



Dashboard.png

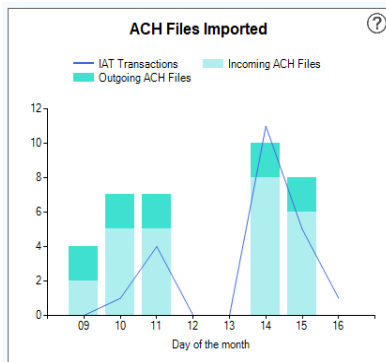
Very important note: The SAM dashboard is referenced in several parts of the Best Practice recommendations. To save space, we will only display one copy of the dashboard.

- Dashboard panels 1 – 5 are the top row, going left to right.
- Dashboard panels 6 – 8 are the bottom row, going left to right.

Daily Best Practice 1—Import all ACH files

Daily Best Practice 1: Import all ACH files (both incoming and outgoing) into SAM

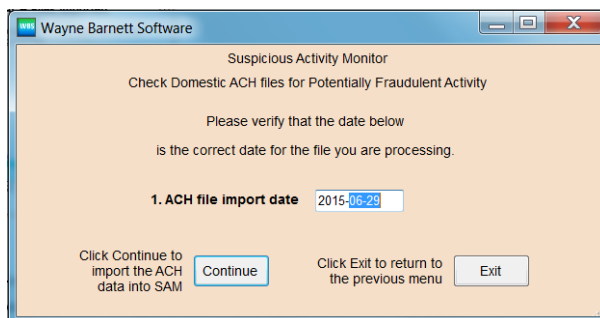
You can import all of your ACH files through the dashboard, by clicking anywhere on a “white area” in dashboard panel 3.



Dbpanel3

1. If I was importing an ACH file for the 16th, I'd click in the white area above the number 16, located on the far right of the “X axis”. (I hated to write the words “X axis”, as it brought back stressful memories of Mr. Sanchez and my high school geometry class.)
2. The screen below will appear. The default date can be either the current day or the prior business day, whichever you prefer.

If you have to change this date each time you import an ACH file, please call us at 469-464-1902 and we'll help fix the issue.



Achimport

3. Click Continue, navigate to the file and double-click on the one you want to import.

Daily Best Practice 1—Import all ACH files

Name	Date Modified	Type	Size
barnett_ctm_demo.bak	11/2/2015 12:13 A...	BAK File	586,618 KB
barnett_dck_demo.bak	11/3/2015 8:38 AM	BAK File	11,866 KB
barnett_ktm_demo.bak	11/2/2015 12:14 A...	BAK File	1,231,198 ...
barnett_wtm_demo.bak	11/2/2015 12:14 A...	BAK File	169,522 KB
demo ach outgoing 2015-06-29.txt	10/5/2015 12:05 A...	Text Document	5 KB

Achfileselect

- If you clicked on the bar graph (the colored part of dashboard panel 3) instead of the white area, you will see a screen like the one shown below. This screen shows all of the files imported on the corresponding day.

	Processing Date *	File ID	In/Out	File Debits *	File Credits *	Number of Batches *	Number of Debits	Number of Credits	WBS File ID# *
▶ 1	2018-06-01	B	Outgoing	\$1,415.41	\$893.60	6	3	2	2018152000003
2	2018-06-01	U	Outgoing	\$10,521.99	\$4,192.67	23	16	6	2018152000004
3	2018-06-01	A	Incoming	\$56,980.09	\$33,093.36	93	116	14	2018152000002
4	2018-06-01	B	Incoming	\$299,261.39	\$229,050.46	302	289	143	2018152000001

achdailyfileselectscreen

Daily Best Practice 2—Analyze Outgoing ACH Files

Daily Best Practice 2: Analyze outgoing files for fraud

Incoming and outgoing files have different fraud-analysis strategies:

- Incoming files are best analyzed when all incoming files for the day have been imported. The reason: to find fraud with incoming transactions, it's best to look at daily totals.
 - A \$5,000 incoming debit may not be unusual for a customer—but if the customer has 3+ \$5,000 debits from the same originator, it will likely raise concern.
 - And since Fed sends your bank at least four ACH files each day (and possibly as many as eight), if multi-transaction fraud is involved, it's likely the transactions will be scattered across several files.
 - By waiting until all incoming files are imported, you decrease the risk of missing transactions that should be comingled.

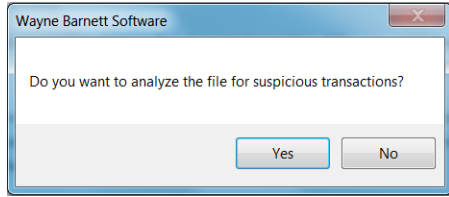
- Outgoing files are analyzed immediately upon importing. Why, you ask? Because we need to know if fraud is involved, prior to forwarding the outgoing ACH file to Fed.
 - Once an outgoing file is sent to Fed, it's gone for good. If you later discover fraudulent transactions in the outgoing ACH file, your only option for stopping the transactions is to contact the receiving depository financial institutions (RDFI).

Note—this strategy seldom works; the funds that were fraudulently conveyed will likely be withdrawn shortly after the receiving bank opens (and before you can contact the RDFI).

- SAM has stopped Corporate Account Takeovers (CATO's) that involved 600+ transactions and 400+ RDFIs. So, again, if your plan for stopping outgoing ACH fraud is to contact the RDFI(s) after the file is sent to Fed ... forget about it (or for our northeast customers, fuggedaboudit).

1. After each file is imported into the system, the screen below appears.

Daily Best Practice 2—Analyze Outgoing ACH Files



Importcheckforfraud

2. Click Yes for outgoing files. Click No for incoming files.
3. The screen below appears, when you click yes.

A screenshot of the 'Suspicious Activity Monitor' window in Wayne Barnett Software. The window title is 'Wayne Barnett Software' and the subtitle is 'Suspicious Activity Monitor'. The main heading is 'Review all ACH Transactions Imported for a Specific Date.' Below this, there are several numbered fields for configuration:

- 1. File processing date: 2019-01-15
- 2. Search criteria: 1. Amount
- 3. Amount range for report - minimum: 100 AND maximum: 9,999,999
- 5. Tolerance level - amount: 120
- 7. Number of months to use for historical compare: 3, 1. Filtered
- 8. Strike zone percentage & number of strikes: 20, 3
- 9. Transactions to review: 7. Outgoing Credits
- 10. Class of transactions to review: 1. Commercial & Consumer
- 11. Sort preference: 4. Tolerance
- 12. Aggregation preference: 1. By Originator

At the bottom, there are two buttons: 'Continue' (labeled 'Click Continue to generate the report') and 'Exit' (labeled 'Click Exit to return to the previous menu').

achdailyreport

- If you are a **Power User (PU)**, you may know enough about SAM to change the parameters on this screen.
- If you don't consider yourself a **PU**, we recommend you leave the parameters as they are, with two exceptions:
 - i. Change minimum amount to \$100.
 - ii. Change field **9. Transactions to review** to **7. Outgoing Credits**.

4. Click continue, the screen below appears.

Daily Best Practice 2—Analyze Outgoing ACH Files

	Account Number ☆	Risk Rating ☆	Name from CIF Record ☆	Name from File	Originators Name ☆	Prior Trans	File Type	Tran Type	Average Amount	Average Trans	Amount	Number Trans	Tol Amount	Tol Trans	Nbr Strikes	DICK ☆
1	2-616-604			Deann Frazier	Oak Alley Founda	7	Outgoing	Credit	\$416.82	1	\$635.44	1	152%	100%	2	
2	895-408			Zeb Mayhew III	Oak Alley Restau	7	Outgoing	Credit	\$927.31	1	\$1,264.38	1	136%	100%	2	
3	4-206-059			Lucas Daigle	Oak Alley Founda	6	Outgoing	Credit	\$703.76	1	\$943.40	1	134%	100%	2	
4	4-244-526			BRANDI CORTEZ	Oak Alley Restau	4	Outgoing	Credit	\$524.49	1	\$695.74	1	133%	100%	1	
5	4-347-101			VICTORIA DESLATTES	Oak Alley Restau	3	Outgoing	Credit	\$278.29	1	\$369.67	1	133%	100%	1	
6	22-633			Jamie Gravois	Oak Alley Founda	1	Outgoing	Credit	\$329.94	1	\$423.56	1	128%	100%	0	

Achdailyreportscreen

- The entries on this report are here because the people getting paid are receiving more money than usual—but the variances are usually not extreme (28-52% above normal).
- I know what you're thinking: **A 52% variance seems extreme to me!** And in some cases you're right. A 52% variance on a \$20,000+ outgoing credit may be fraudulent. But, a 52% variance on a \$635 outgoing credit is fairly common.
- As a rule, we recommend you ignore all outgoing credit transactions where the dollar amount is less than \$5,000—unless it's a first-time transaction.
 - i. If it's a first-time transaction for more than \$3,500, we recommend you confirm the transaction with the customer.
 - ii. If the tolerance level is 300% or more (that is, if the dollar amount of today's transaction(s) is 3x more than the recipient normally receives), and the total dollar amount to the recipient is \$5,000 or more, the transaction should be confirmed with the customer.
 - iii. If the tolerance level is 200% - 299% (that is, if the dollar amount of today's transaction(s) is 2x – 3x more than the recipient normally receives) and the dollar amount is \$10,000 or more, the transaction should be confirmed with the customer.
 - iv. If the tolerance level is 150% - 199% and the dollar amount is \$20,000 or more, the transaction should be confirmed with the customer.

Important note: You're probably wondering why we looking at small dollar amounts, if we aren't concerned about large variances in small dollar amounts? The answer: **Corporate Account Takeover (CATO) losses.**

A CATO loss happens when the outgoing ACH file is intercepted by hackers and all credit transactions are rerouted to "hacker-controlled bank accounts". What's a "hacker-controlled bank account"? Let me give you an example: When my wife and I travel, we normally find a laundromat early Sunday morning and do our clothes. In a great many laundromats, you'll find advertisements where people are promised \$15 a month for life, if they will open a bank account for the advertiser. The advertiser will send the unsuspecting accomplice (UA) a money order for \$30, to be used to open the account. The UA will open the account, setup the account with Bill Pay rights and take his initial \$15. The advertiser will sell access this account to a hacker group for \$100, and the hackers can now commit their frauds. Specifically, they'll use a CATO to move money into the account and a Bill Pay transaction to move it out.

Daily Best Practice 2—Analyze Outgoing ACH Files

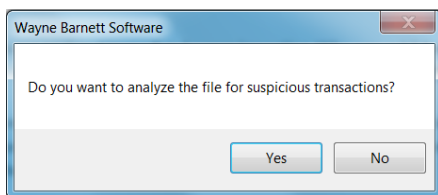
The average CATO transaction is \$430, but a great many of the CATO transactions will be less than \$300. So, we recommend you set your minimum amount at \$100.

5. If you have a CATO situation, the report screen will look something like this.

	Account Number ★	Risk Rating ★	Name from CIF Record ★	Name from File	Originators Name ★	Prior Trans	File Type	Tran Type	Average Amount	Average Trans	Amount	Number Trans	Tol Amount	Tol Trans	Nbr Strikes	DiCK ★
1	153-036-214			Wayne Barnett	H. WAYNE BARNETT	0	Outgoing	Credit	0	0	\$300,055.25	1			0	
2	1000084-644-136			Maureen Otoole	H. WAYNE BARNETT	0	Outgoing	Credit	0	0	\$70,004.98	1			0	
3	5711-589-701			Henry G. Utley, MD	H. WAYNE BARNETT	0	Outgoing	Credit	0	0	\$3,920.63	1			0	
4	3-007-524			David Sweat, Kay Giese	H. WAYNE BARNETT	0	Outgoing	Credit	0	0	\$3,588.55	1			0	
5	334008-323-874			Oglethorpe 295 LLC	H. WAYNE BARNETT	0	Outgoing	Credit	0	0	\$1,917.79	1			0	
6	334008-323-222			Meigs 570 LLC	H. WAYNE BARNETT	0	Outgoing	Credit	0	0	\$1,600.00	1			0	
7	5536-444-678			Hammerland Investment	H. WAYNE BARNETT	0	Outgoing	Credit	0	0	\$1,593.50	1			0	
8	58-856-977			Sidney M. Newman	H. WAYNE BARNETT	0	Outgoing	Credit	0	0	\$1,235.00	1			0	
9	334033-151-501			Himansu I Bhavsar	H. WAYNE BARNETT	0	Outgoing	Credit	0	0	\$1,192.50	1			0	
10	1003225-756-246			Michelle M. Carney	H. WAYNE BARNETT	0	Outgoing	Credit	0	0	\$1,013.38	1			0	
11	1000027-519-585			Jason Eller	H. WAYNE BARNETT	0	Outgoing	Credit	0	0	\$961.91	1			0	
12	65004-937-110			Ronald & Julia Moye	H. WAYNE BARNETT	0	Outgoing	Credit	0	0	\$952.34	1			0	

Achdailyreportscreen-cato

- The easiest way to identify a CATO is to look at the “Average Amount” field on the report. If most or all of the transactions on the report show a \$0 Average Amount, one of two things has happened:
 - 1) The ACH file-originator is a new customer, and this is the first payroll file he’s sent to the bank.
 - 2) Or, your customer’s PC has been compromised and a CATO has occurred.
 - If your bank forwards an ACH file to Fed, and that file has been compromised with a CATO, the loss could be significant for your bank. (Under current case law, customers are not responsible for CATO losses.)
 - I hate to say that sending a compromised ACH file to Fed is a career-killer ... but I’m pretty sure it is. So, please make sure you and the people working for you know how to spot a compromised ACH file.
6. After you review the file for suspicious transactions, the system will ask if you want to check the file stats (that is, number of transactions & total dollar amounts) with past files from this originator.



Importcheckforfilestats

- We always recommend you reply Yes, just to double-check that everything looks normal. The screen below will appear.

Daily Best Practice 2—Analyze Outgoing ACH Files

Wayne Barnett Software
achbatchcompare
Suspicious Activity Monitor

Review of ACH Batches for Normality

1. Company ID, File ID or ALL: 2015177000090

2. File processing date: 2015-06-26

3. Number of months to use for historical compare: 3

4. Tolerance level: 120

5. Minimum amount: 7,500

6. Type of files to show: 3. Outgoing only

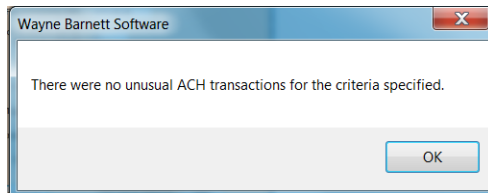
7. Type of transactions to show: 1. All

8. Sort preference: 1. Originator-ID

Click Continue to generate the report Click Exit to return to the previous menu

Achbatchcompare

- This screen instructs the system to do the following:
 - Show all batches in this file where the total debits or total credits is \$7,500 or more, and, the amount is at least 20% above the averages.
 - Calculate the averages, based on the ACH transactions the customer has sent to the bank in the last three months.
- Most of the time, you'll see a message like the one shown below (which says that everything looks normal).



Achbatchcompare-nodata

- On occasion, you may be advised that a batch is slightly larger than normal. The report below shows how this information is presented.

Wayne Barnett Software
achbatchcomparescreen
Suspicious Activity Monitor

Comparison of Outgoing Transaction Batches with Prior Days

For Company ID# All on 2018-05-11, Compared to Files from 2018-02 to 2018-05

Amounts >= \$500.00, Tolerance Level = 120%

	File Type	Originator ID Number ☆	Originator Name	Tran Type	Day's Amount	Day's Number of Items	Average Amount	Average Items	Tol Amount	Tol Items
▶ 1	Outgoing	756019458	JOHNS CAKE STORE	Credit	\$217,956.00	82	\$167,873.25	81	130%	101%

Achbatchcomparescreen

Daily Best Practice 2—Analyze Outgoing ACH Files

Very important note #1: Please make sure you understand the difference between an ACH batch and an ACH file.

- When a customer directly sends the bank an ACH file, that file will usually have just one batch. So, in this instance, the words “batch” and “file” can be used interchangeably.
- When your customer sends the ACH file to you via the Internet Banking System, (IBS), the words “batch” and “file” are no longer interchangeable.
 - All ACH files sent to your bank via the IBS are stripped-down to the batch-level, and stacked together.
 - So, that single ACH file you receive from the IBS may contain transactions from a dozen (or more) originators. (That is, it may have a dozen or more batches, in a single file. Or to put it another way, a dozen outgoing ACH files were combined into a single file, and reformatted per NACHA rules.)
 - Why does the IBS reformat the ACH files? Why does it combine 12 (or more) files into one? The answer: money. It will cost \$16/day to send 12 separate files to Fed, but less than \$1.40/day to send a single file.

Very important note #2: If you have any doubts about the legitimacy of outgoing credits, try to verify the transaction(s) with the originating party prior to sending the outgoing file to Fed.

- If the customer says the transaction is fraudulent, it must be stripped from the file, prior to sending the file to Fed.
 - We can help you with this, but, we will need to set up your bank for it, which will require written permission from a senior bank officer (that is, President, CFO, or SVP) prior to doing so.
- If the customer can't be contacted because the file came late in the day, be sure to have someone contact them first thing the next morning (as early as possible).
 - If the customer says the transactions are fraudulent, immediately contact the receiving bank(s) and ask them to put holds on the deposits.

Note—as previously noted, there could be hundreds of receiving banks. So, bottom line: this is a move of desperation and should only be done as a last resort.

Daily Best Practice 2—Analyze Outgoing ACH Files

- Please realize the RDFI has no legal obligation to put a hold on the fraudulent transactions you sent to them—so we recommend that a senior bank official contact the RDFI and politely ask (or beg) for their help.
- In a worst-case scenario, you can use the “nuclear option”. That is, you can strip the transaction(s) from the file, without the customer confirming they are fraudulent.
- Using the “nuclear option” is very risky. It could create a breach of contract with your customer. It may also create a violation of law for unauthorized dishonorment.
- But if we were working at a bank and saw a large suspicious transaction we couldn’t verify, we’d strip that sucker out in a heartbeat.
- ❖ This would be especially true if the RDFI was in an earlier time zone (that is, if the receiving bank opens for business before we do). If the RDFI begins its business day while we’re still having breakfast, there’s a chance the funds will be withdrawn before we get to work.
- ❖ Once the funds are gone from the receiving bank, there’s nothing more you can do. If the transaction was in fact fraudulent, the sending bank has a loss.

Note—you can ascertain where the RDFI is located by entering their routing transit number into Google.

- ❖ If the transaction was legit, you can deliver the funds immediately via a wire transfer. This effectively negates the nuclear option. The funds arrive an hour or two later—but still on the same business day.
- 7. After you have completed your review of outgoing credits, repeat all of the same steps for outgoing debits.**
- Keep the search parms (that is, the dollar amount, tolerance level and number of prior months to include for historical compare) the same. Change field **9. Transactions to include** to **6. Outgoing Debits**.
 - Outgoing debits are less risky than outgoing credits, because the bank is not sending money out the door.
 - However, all outgoing consumer debits are unconditionally guaranteed by the bank for four years.

Daily Best Practice 2—Analyze Outgoing ACH Files

- So, if a health club owner or apartment complex manager wants to steal from their customers by double or triple billing them, they can do so by sending fraudulent ACH debits. And once this theft is discovered, if the health club or apartment owner is unable to reimburse the injured parties, the bank is liable for the injuries (e.g., the stolen funds and any damages the victims incurred, due to their funds being illegally taken).
- What's that you say? You thought the warranty period was 60 days? Well, trust us, that's not the case. A lot of consultants and auditors think that, but they are wrong.
 - i. NACHA rules, Article 2 Subsection 2.4.5.1 states that an ODFI will warrant the legitimacy of all outgoing debit transactions. The rules don't specify a warranty period; rather, the warranty period is prescribed by the laws of the state where the transactions originated.
 - ii. The Uniform Commercial Code (UCC) covers payment warranty in Article 2 Section 275. The normal warranty period is four years.

Bottom line: your bank could have been a victim of this crime 47 months ago and you'd still be liable for the loss.

- ACH debit fraud is highly unusual; we've only seen it 2-3 times. But when it happens, the losses can be huge (\$500,000 or more). Years ago, the first Internet Bank was named Wingspanbank.com. It was closed two years after opening, partially due to a large ACH debit fraud. (Note: Wingspan was part of the Bank One holding company, Chicago, IL. Bank One made all the victims whole and moved Wingspan's customers to Bank One.)
 - One small bank in Delaware was also fined \$1 million by the regulators, for not doing enough to prevent fraudulent outgoing ACH transactions. That bank did not close, but, due to a lack of capital it was forced to sell.
- So, bottom line: this is a procedure you need to do daily. But, don't be surprised if you never see ACH debit fraud; it seldom happens. And the good news: this daily check will usually take just 1-2 minutes a day.
- Here are the review procedures we recommend:
 - i. If the **total** of first-time debits is \$5,000 or more, the transactions should be confirmed with the customer and proof of authorization should be obtained.
 - ii. If the tolerance level is 300% or more (that is, the size of the debit is 3x larger than normal), and the **total** dollar amount is \$5,000 or more, the transactions should be confirmed with the customer and proof of authorization should be obtained.

Daily Best Practice 2—Analyze Outgoing ACH Files

- iii. If the tolerance level is 200% - 299% (that is, the size of the debit is 2x – 3x larger than normal), and the **total** dollar amount is \$10,000 or more, the transactions should be confirmed with the customer and proof of authorization should be obtained.
- iv. If the tolerance level is 150% - 199% and the **total** dollar amount is \$20,000 or more, the transactions should be confirmed with the customer and proof of authorization should be obtained.

Daily Best Practice 3—Analyze Incoming ACH Files

Daily Best Practice 3: Analyze incoming files for fraud

As noted in the prior section, you want to import all incoming files, prior to checking for fraud. Why is that, you ask? It's because, unlike outgoing files, we don't want to check individual incoming transactions. Rather, we want to check total incoming transactions, by account, based on the originator. Please let me explain with an example:

- Barnett's Po Boy sandwich shop receives a \$5,000 incoming ACH debit from Rudolph's Meat Market. This transaction is not unusual; Rudy sends the Po Boy shop one of these transactions every week, for amounts ranging between \$4,500-\$5,500.
 - But let's suppose Rudy is having refrigeration problems and needs to raise money. And, let's suppose the stress of the situation causes Rudy too inadvertently (... or maybe purposely) bill the Po Boy shop three times—each for \$5,000.
 - And, let's say Rudy does the transactions at different times, so that each of the three \$5,000 ACH debits arrive in a different file from Fed.
 - If we check each file separately, we won't spot the overcharge. But, if we check for fraud after all files are imported, the additional \$10,000 that Rudy billed will be extremely obvious.
 - What's that you ask? Why do we have to check for such fraud? I mean, after all, it's the Po Boy shop that's being stolen from—not the bank. But under UCC Article 4A, the customer can dispute the transactions—possibly as long as five weeks after they posted—and now the bank has the loss. Oh ... and forget about trying to return the transactions. Since these are commercial ACH transactions, the return is one day. The 60-day rule only applies to consumer transactions.
1. Dashboard panel 8 (lower level, last panel on the right) has links to the eight most-used ACH reports. Please click on the first report (Report #7502). The screen below will appear.

Daily Best Practice 3—Analyze Incoming ACH Files

ACH Reports Status			
Nbr	Report Name	Status ☆	Total Time In Report
7502	Daily ACH Report	Reviewed ✓	0.47 Minutes (Today)
7550	Daily 1,000-Cuts Report	Reviewed ✓	1.33 Minutes (Today)
8012	Daily IAT Report	Missing ✕	0 Minutes (Today)
7503-7505	Account ACH Reports	Missing ✕	0 Minutes (Today)
8003	Monthly IAT Report	Missing ✕	0 Minutes (Last 30-days)
7701	Monthly Orig Name Search	Missing ✕	0 Minutes (Last 30-days)
7507	Monthly High Activity	Missing ✕	0 Minutes (Last 30-days)
7514	Monthly Govt Benefits	Missing ✕	0 Minutes (Last 30-days)

Dbpanel8

Achdailyreport-in

2. Most of the search-variables will not change, because they're set as system parms. Here's our recommendations for setting the system parms.
 - 1) **3. Minimum dollar amount** – banks up to \$100 million in assets, set this value at \$2,500. Increase the value by \$500 for each additional \$100 million in assets, with a maximum value of \$7,500.
 - 2) **5. Tolerance level** – 120. Any transaction that's more than 20% above the average should be flagged for review.
 - 3) **7. Number of months to use for historical compare** - 3. What this field does is look at ACH transactions for the past "xx" months, (for example, three months) and determine the average daily transactions an originator sends to a bank's customers.

Daily Best Practice 3—Analyze Incoming ACH Files

Some banks use 2 past months, some banks use 6. We recommend 3 past months; we've found that three past months creates less-skewed data.

- 4) **8. Strike zone percentage & number of strikes.** These parms tell the system to exclude reportable transactions, if the customer has a history of similar transactions. We recommend settings of 20 and 3.

How do we define similar transactions? When the parms are set at 20 and 3, a transaction is considered similar when:

- 1) There have been three or more days in the past month where a specific originator sent transactions to our customer, and
 - 2) The total transactions for three or more of those days were within 20%, above or below, the amount sent today.
- 5) **9. Transactions to review** – We recommend setting this at **8. Incoming Debits**, since the focus on this procedure is finding unauthorized withdrawals from our commercial customers.

Leave all other variables unchanged, unless you consider yourself a Power User (PU).

3. The report shown below is produced.

	Account Number ☆	Risk Rating ☆	Name from CIF Record ☆	Name from File	Originators Name ☆	Prior Trans	File Type	Tran Type	Average Amount	Average Trans	Amount	Number Trans	Tol Amount	Tol Trans	Nbr Strikes
1	4-173-059	C 0	Blue Ocean Bank ...	BLUE OCEAN BANK	HarlandClarkeCar	21	Incoming	Debit	\$1,409.31	1	\$71,750.70	1	5091%	83%	0
2	4-110-926	C 0	84 LUMBER COMPA...	84 LUMBER COMPANY	84 LUMBER CO	61	Incoming	Debit	\$20,745.75	1	\$186,803.09	1	900%	91%	0
3	23-074	C 0	RIVERLANDS INSUR...	RIVERLANDS INSURANCE	UPC INSURANCE	187	Incoming	Debit	\$3,068.95	2	\$11,153.00	3	363%	176%	1
4	95-343	C 0	ALLIANCE INSURAN...	ALLIANCE INSURANCE AGE	UPC INSURANCE	187	Incoming	Debit	\$2,772.42	1	\$9,989.00	3	360%	231%	0
5	23-074	C 0	RIVERLANDS INSUR...	RIVERLANDS INS SVC	ORCHID PREMIUM	7	Incoming	Debit	\$81,754.52	1	\$168,818.45	1	206%	100%	0
6	9-108-091	C 0	MICHAELA CARAVE...	MICHAEL CARAVELLA	CHASE	2876	Incoming	Debit	\$13,014.29	1	\$22,306.78	1	171%	77%	1
7	4-420-224	C 0	RODNEY P SALVAG...	RODNEY SALVAGGIO	AMEX EPayment	1492	Incoming	Debit	\$20,258.74	1	\$30,210.11	1	149%	100%	0
8	4-228-070	C 0	SUPREME TIRE SER...	DOUGLAS J OHMER JR	MASTERCARD	447	Incoming	Debit	\$5,209.36	1	\$7,518.39	1	144%	100%	1
9	4-302-892	C 0	ZEESHAN SYED ...	SYED	DISCOVER BANK	81	Incoming	Debit	0	0	\$23,472.12	1			0
10	9-064-827	C 0	DR ELSA MATHERN...	580821973617265	CHASE	2876	Incoming	Debit	0	0	\$11,000.00	1			0
11	4-348-355	C 0	MARCELLO DISTRIB...	MIKE M MARCELLO INC	MOTIVA ENTE 3038	82	Incoming	Debit	0	0	\$9,214.23	1			0

Achdailyreportscreen-in

4. There are five things we're looking for with this report:

- 1) **First-time transactions (that is, those that have zero in the Average Amount) that do not look to be authentic. How do you determine authenticity?**

- i. Look at the prior transactions the originator has sent to the bank, in the past three months (that's the column labeled **Prior Trans**). If that number is above 50, you've passed test #1. (For a smaller bank, 20 may be a suitable number of prior transactions.)
- ii. Look to see if the name from the file matches the name from the CIF record. If the names appear to reference the same business or person, you've passed test #2.

Daily Best Practice 3—Analyze Incoming ACH Files

- iii. Look at the dollar amount. If it is less than 3x the search amount (in this example, our search amount was \$7,500—so 2x that amount is \$15,000), we passed test #3.

If a first-time transaction passes all three tests, we'll not take any further action. If it doesn't pass all three tests, you should contact the customer and verify the transaction's authenticity.

2) Transactions that are not first-time, and, where the name from the file is different from the CIF record.

- i. When the names don't match, click on the Account Number and then click Continue. This will show you all transactions this originator has sent our customer, for the last three months.
- ii. If the originator has sent us transactions every month for the last three months, and, the total dollar amount of the transactions today is less than 2x the search amount, we'll take no further action. However, if we don't pass both tests (a history of monthly transactions and less than 2x the search amount, you should contact the customer and verify the transaction's authenticity.

3) Transactions that are not first-time and where the originator has sent fewer than 20 additional transactions to the bank, in the past three months. (The column labeled **Prior Trans** shows how many additional transactions the originator has sent in the past three months.)

- i. Click on the Account Number and then click Continue. This will show you all transactions this originator has sent our customer, for the last three months.
- ii. If the originator has sent us transactions every month for the last three months, and, the total dollar amount of the transactions today is less than 2x the search amount, we'll take no further action. However, if we don't pass both tests (a history of monthly transactions and less than 2x the search amount, you should contact the customer and verify the transaction's authenticity.

4) Transactions that are not first-time and that have a Tolerance Level of 200% or more.

- i. Click on the Account Number and then click Continue. This will show you all transactions this originator has sent our customer, for the last three months.

Daily Best Practice 3—Analyze Incoming ACH Files

- ii. If the originator has sent us transactions every month for the last three months and one of the following two conditions is present, we'll take no further action. The two conditions are:
 - a) There's at least one strike (that is, one day with transactions close to what we received today). The column labeled **Nbr Strikes** shows this information.
 - b) The originator has sent the bank 500 or more transactions in the past three months. (For a smaller bank, 150 prior transaction is probably adequate.)

However, if we don't pass both tests (a history of monthly transactions, and, 1 or 2 strikes with a suitable number of prior transactions), you should contact the customer and verify the transaction's authenticity.

5) Transactions that are not first-time and are 5X the search amount.

- i. If there's two strikes, and, the originator has sent the bank 500 or more transactions in the past three months, we'll not take any further action. If both of these tests aren't passed, you should contact the customer and verify the transaction's authenticity. (For a smaller bank, 150 prior transactions is probably adequate.)

Very important note #1: The return period for unauthorized commercial ACH transactions is just two business days.

- **Commercial ACH transactions are not covered by Reg E, so they don't have the 60-day unconditional return period prescribed by NACHA, or, the four-year return period mandated by UCC-2.**
 - **Also, in most instances, the originator of commercial ACH transactions is not required to have written authorization from the company that's being debited. If the originator will sign an affidavit stating the party being debited verbally authorized the commercial transaction, the transaction is considered legally authorized.**
 - **As a side note, the determination of authorization can be voided by the courts. However, under NACHA rules for a commercial transaction, any litigation to void a verbal authorization must be filed in the state where the transaction originated.**
 - **Also, per NACHA rules, the plaintiff is required to pay all legal and court costs of the defendant, if the court rules in favor of the defendant.**

Daily Best Practice 3—Analyze Incoming ACH Files

- But please don't think that ODFI's have minimal risk from accepting returned commercial transactions. That is not the case. If a commercial ACH transaction is being returned to your bank, proceed with caution.
 - You cannot automatically assume that your customer is at fault. If your customer has written authorization for the commercial ACH transactions and you accept the return, your bank can be sued for illegal dishonorment of a transaction.
 - If your customer can't provide written proof of authorization and the transaction is returned within the two-day window, you can probably accept the return without issue. (We can't think of a reason why you couldn't accept a commercial ACH transaction that was returned within two-days of posting; but, each state has its own laws so check with your bank's legal counsel first).
 - If you accept a returned commercial ACH transaction after more than two days and your customer is willing to sign an affidavit stating the transaction was authorized, you can again be sued for illegal dishonorment of a transaction.
 - Bottom line: on the fourth day after your bank accepts an outgoing commercial ACH transaction from your customer, don't accept a returned transaction—unless your customer says it's OK.
- 6. After you have completed your review of incoming ACH debits, you should quickly review incoming credits.
 - Incoming credits pose little risk of loss to the bank. In all honesty, if someone is sending me money, I'm not greatly concerned.
 - But there is one scenario where receiving money can create problems: if you have a customer receiving multiple credits each month, even if just from one source, you need to know what the customer is doing. There have been hundreds of instances in the past few years where criminals and terrorist used ACH transactions to launder money disbursed through private ATMs. This money-laundering scheme is becoming so common that the FBI issued an alert on it in 2016.
 - Keep the search parms (that is, the dollar amount, tolerance level and number of prior months to include for historical compare) the same as incoming debits. Change field **9. Transactions to review** to **9. Incoming credits**.
 - Here are the review procedures we recommend:

Daily Best Practice 3—Analyze Incoming ACH Files

- i. All first-time credits shown on the report should be confirmed with the receiving party, unless you know the customer well.
 - ❖ We don't expect the bad guys to confess to their crimes and immediately turn themselves in to the police; but if they know they're being watched they may move to a less conscientious bank.
- ii. All credits at or above the bank's "large-item amount" should be confirmed with the **originating party (you'll need the ODFI's help for this chore)**, if the tolerance level for the transaction is 0 (that is, a first-time transaction) or above 200%.
- iii. If a large incoming credit can't immediately be confirmed by the ODFI or the originator, it should be held by the bank.
 - ❖ Banks have been found liable of contributory negligence, when they knowingly allowed a large and unusual deposit to be immediately withdrawn from the bank.
 - ❖ Over the past ten years, we've seen 11 instances where small transactions had two additional zeroes added. These transactions are almost always tied to retirement accounts, estate settlements or employment severance payments. The largest error we've seen was by a school district that was supposed to pay severance of \$9,100. Instead, the payment the bank received was \$910,000. The bank would not release the deposit until the school sent a confirmation letter—and the school district did just that. But ... the bank was still dubious and called the district superintendent.

The superintendent immediately asked the bank to hold the transaction, and later confirmed it was an error. The person whose account was almost credited for an extra \$900,000 screamed and threatened the bank throughout the two days it took to resolve this. After the customer's account was properly credited, she was asked to close her account.

Now, we know what you're thinking: the person who sent the confirmation letter—were they part of a scheme to steal from the school district? The police thought so, but nothing could be proved. He was fired for cause.

Daily Best Practice 4—Search for Pink Cowboy Boots Fraud

Daily Best Practice 4: Search for Pink Cowboy Boots Fraud

Individual Account Takeover (IATO) has become one of the most common forms of fraud perpetrated against individual customers who are over the age of 50. It's estimated that in 2019, one in four banks will have a customer who experiences a significant financial loss from an IATO.

How, you ask, does an IATO occur? Let us please explain with a true story from a bank in CO.

- i. A woman in Colorado meet a man in Georgia on an over-50 dating site and soon they became good friends.
- ii. After a few months of skyping, the man asked the woman for a favor: would she please buy his granddaughter a pair of cowboy boots from a nearby specialty store. He'd send her \$300 for the boots and postage, and an additional \$50 for her trouble. She agreed to help.
- iii. A week later, the man asked if she'd received the check and she replied no.
- iv. The man was mortified—his granddaughter's birthday was ten days away! He asked her permission to deposit the funds directly into her account. The woman at first refused but later acquiesced, after the man convinced her there was no risk.
- v. Two days later, the man called to confirm the woman had received the funds, and she again said no. She told him there were three small transactions that may be from him: a \$.07 deposit and two withdrawals of \$.03 and \$.04—but nothing else. The man humbly apologized and promised to contact his bank right away.
- vi. The woman never heard from the man again. In November 2018, she was reconciling her bank account for the first time in several months (getting ready for Christmas, don't you know) and found that \$41,000 was missing. The withdrawals had happened in August, two months after she and the man quit speaking.
- vii. The woman's bank tried to return the withdrawals, but the originating bank denied their request, citing the NACHA 60-day rule. The woman's bank then tried to return the funds under UCC-2.275. The originating bank again said no: they considered the transactions authorized by the victim. (Also, the account that received the funds was closed.)

"We had two choices," said the BSA officer at the victim's bank: "Express our sympathy for the customer's misfortune and suffer bad publicity—we'd already been contacted by a local TV station. Or, make the customer whole and buy software that will help us prevent this in the future. We chose the latter."

Daily Best Practice 4—Search for Pink Cowboy Boots Fraud

1. Dashboard panel 8 (lower level, last panel on the right) has links to the eight most-used ACH reports. Please click on the first report (Report #7502). The screen below will appear.

Nbr	Report Name	Status ☆	Total Time In Report
7502	Daily ACH Report	Reviewed ✓	0.47 Minutes (Today)
7550	Daily 1,000-Cuts Report	Reviewed ✓	1.33 Minutes (Today)
8012	Daily IAT Report	Missing ✕	0 Minutes (Today)
7503-7505	Account ACH Reports	Missing ✕	0 Minutes (Today)
8003	Monthly IAT Report	Missing ✕	0 Minutes (Last 30-days)
7701	Monthly Orig Name Search	Missing ✕	0 Minutes (Last 30-days)
7507	Monthly High Activity	Missing ✕	0 Minutes (Last 30-days)
7514	Monthly Govt Benefits	Missing ✕	0 Minutes (Last 30-days)

Dbpanel8

Achdailyreport-iato

2. Most of the search-variables will not change, because they're set as system parms. Here's our recommendations for setting the system parms.
 - 1) **3. Minimum dollar amount** – \$0.01.
 - 2) **3. Maximum dollar amount** - \$2.00
 - 3) **5. Tolerance level** – 120. Any transaction that's more than 20% above the average should be flagged for review.

Daily Best Practice 4—Search for Pink Cowboy Boots Fraud

- 4) **7. Number of months to use for historical compare** - 3. What this field does is look at ACH transactions for the past “xx” months, (for example, three months) and determine the average daily transactions an originator sends to a bank’s customers.

Some banks use 2 past months, some banks use 6. We recommend 3 past months; we’ve found that three past months creates less-skewed data.

- 5) **8. Strike zone percentage & number of strikes**. These parms tell the system to exclude reportable transactions, if the customer has a history of similar transactions. We recommend settings of 20 and 3.

How do we define similar transactions? When the parms are set at 20 and 3, a transaction is considered similar when:

- 1) There have been three or more days in the past month where a specific originator sent transactions to our customer, and
- 2) The total transactions for three or more of those days were within 20%, above or below, the amount sent today.

- 6) **9. Transactions to review –1. All transactions.**

Leave all other variables unchanged, unless you consider yourself a Power User (PU).

3. The report shown below is produced.

Name from CIF Record	Name from File	Originators Name	Prior Trans	File Type	Tran Type	Pass/Fail Score	Average Amount	Average Trans	Amount
DIXIE LOWREY	DIXIE LOWREY	eBay Inc.	0	Incoming	Debit	Fail-2	0	0	\$1.88
NANTZ EXTERIORS LLP	NANTZ EXTERIORS LLP	Kimberly Clark C	0	Incoming	Credit		0	0	\$10
EDITH GALLO	GREG LATOUR	PAYPAL	0	Incoming	Debit	Fail-3	0	0	\$0.07
EDITH GALLO	GREG LATOUR	PAYPAL	0	Incoming	Credit		0	0	\$0.07

Achdailyreportscreen-iato

4. There are three things we’re looking for with this report:

- 1) The name from the file and the name on the account do not match.

- i. We’re assuming the entries on this report show which of your customers are trying to access their account at your bank, from their account at another bank.

When the names don’t match, you have to assume that someone else is trying to access your customer’s account. This type of theft becomes even more suspicious when the originator is PayPal.

- 2) The total debits and credits equal and are typically less than \$0.25.

Daily Best Practice 4—Search for Pink Cowboy Boots Fraud

This scenario is almost always an attempt by a bank or FinTech to authenticate that their customer has transaction-authority for an account at your bank.

- 3) Check the age of the customer. According to AARP magazine, the majority of people over the age of 50 do not reconcile their bank statements.

Not that we read AARP magazine ... OK, yes, we do—but only for the recipes!

If you think you have an IATO, contact the customer immediately and ask if they have given their account information to anyone. Also advise them not to mention the two “confirming transactions” to anyone. And, use the KYC risk-factor to mark this account as super-high risk.

One last thing: if the customer is wealthy, consider closing the account and opening a new one. Tested IATOs (that is, accounts that have been successfully stolen from) often sell for thousands of dollars on the dark web. The criminals willing to spend this much expect to successfully steal tens-of-thousands of dollars—and that’s what happened to the woman in CO.

Daily Best Practice 5: Search for 1,000-Cuts Fraud-

A \$450 loss from a fraudulent transaction is annoying but not overwhelming. All banks have a few such losses every year. But suppose it wasn't just one loss: suppose it was 20 ... or maybe 50 ... or maybe even 200 losses ... and suppose they all happened over 10 days. This fraud, known as "death by a thousand cuts", is happening to banks all over the country. We discuss it below.

1. Thieves will identify a small number of commercial customers at your bank. For example:
 - a) 10-15 customers at a bank with \$100 million in assets.
 - b) 50-75 customers at a bank with \$500
 - c) And the numbers keep going up from there.

Note: we're often asked: "How do thieves identify their targets?" The answer: the people attacking your bank are part of domestic and international organized crime groups. For years, they've collected commercial checking account information from small check-cashers (for example: convenience stores, liquor stores, independent check-cashers and pay day lenders). In many instances they own the businesses where people cash their payroll checks. They also use hacking techniques, bribes and threats to get the data they want.

2. After the bank and accounts are selected, the thieves will create dozens of ACH debits.
 - a) Each targeted account will be debited 2-3 times, over 5-10 days.
 - b) The thieves' strategy is to make the transactions small enough that they aren't immediately reviewed.
 - 1) The transactions typically range from \$400 - \$650.
 - 2) The thefts usually aren't brought to the bank's attention until after the customer's next statement arrives—and that's typically 10-15 days after the theft.
 - 3) By that time, the transactions can't be returned. (Commercial ACH transactions are not covered by Reg E. Accordingly, their return period is two (2) days, not 60.
 - 4) At this point the bank has two options: sue the originator or take a loss.
 - i. Under NACHA rules, any suit brought by an RDFI against an originator has to be filed in the state where the ODFI resides—and that means the suit is likely to be expensive.
 - ii. NACHA rules also require the loser of the suit (that is, the RDFI or the originator) to pay all legal and court costs for both parties.
 - iii. In most instances, the states where commercial ACH transactions originate do not require written authorization from the transaction-recipient. (Again, please remember that Reg E does not apply to commercial ACH transactions.) Accordingly, there's little likelihood that an RDFI will successfully pursue litigation.
 - iv. Most banks, after consulting with legal counsel, decide to accept a loss.

Daily Best Practice 5—Search for 1,000-Cuts Fraud

So, how do you successfully combat thousand-cut fraud? You look for first-time incoming ACH debits, or, ACH debits that are much larger than usual.

1. Dashboard panel 8 (lower level, last panel on the right) has links to the eight most-used ACH reports. Please click on the second report (Report #7550). The screen below will appear.

Nbr	Report Name	Status ☆	Total Time In Report
7502	Daily ACH Report	Reviewed ✓	0.47 Minutes (Today)
7550	Daily 1,000-Cuts Report	Reviewed ✓	1.33 Minutes (Today)
8012	Daily IAT Report	Missing ⚠	0 Minutes (Today)
7503-7505	Account ACH Reports	Missing ⚠	0 Minutes (Today)
8003	Monthly IAT Report	Missing ⚠	0 Minutes (Last 30-days)
7701	Monthly Orig Name Search	Missing ⚠	0 Minutes (Last 30-days)
7507	Monthly High Activity	Missing ⚠	0 Minutes (Last 30-days)
7514	Monthly Govt Benefits	Missing ⚠	0 Minutes (Last 30-days)

Dbpanel8

Wayne Barnett Software

Suspicious Activity Monitor

Search for Originators with an Unusually High Number of Transactions

1. ACH analysis date: 2019-01-15

2. ACH analysis period (in months): 3

3. Type of ACH file: 1. Incoming

4. Type of transactions: 1. Debits only

5. Account type: 1. Commercial only

6. Minimum transaction amount: 400

7. Minimum number of transactions: 1

8. Minimum growth percentage for the day: 50

9. Sort preference: 1. Amount

Click Continue to generate the report: Continue

Click Exit to return to the previous menu: Exit

Achoriginatoridnumberoftransactions

2. Most of the search-variables are self-explanatory and they will seldom change (because they're set as system parms). Below we describe the system parms that have the potential to be most confusing.
 - 1) **5. Account type** – 1. Commercial only. We aren't overly concerned about Consumer transactions, because Reg E gives us 60 days to return them
 - 2) **6. Minimum transaction amount** - \$400. As noted above, a 1,000-cut loss involves dozens of small transactions, posted over a small number of days.
 - 3) **7. Minimum number of transactions** – 1

Daily Best Practice 5—Search for 1,000-Cuts Fraud

- 4) **8. Minimum growth percentage for the day – 50.** What this field does is look at ACH transactions for the past “xx” months, (for example, three months) and determine the average daily transactions an originator sends to all of the bank’s customers.

If an originator sent any transaction that is 50% larger than usual, or, if total transactions from the originator are 50% larger than normal, the customer will appear on this report.

3. The report shown below is produced.

	Processing Date	File Type	Originator ID#	Originator Name	ODFI	Debit/Credit	Days Amount	Days Items	History Amount	History Items	Amt Pctg	Items Pctg	History Days
▶ 1	2019-01-15	In	9500000000	BK OF AMER VIMC	12114128	Debit	11,347.38	2	5,373.00	1	211	200	14
2	2019-01-15	In	9279744991	CAPITAL ONE	05140551	Debit	7,288.98	1	4,297.00	1	170	100	33
3	2019-01-15	In	7232240321	WESTGUARD INS CO	09100001	Debit	1,311.00	1	.00		9,999	9,999	

achoriginatoridnumberoftransactionsscreen

4. There are three things we’re looking for with this report:

- 1) **First time transactions.**

Businesses seldom get “first time transactions”. (That is, an originator sending an ACH debit to a commercial customer for the first time.)

- 2) **Transactions that are much larger than usual.**

This scenario usually indicates a mistake on the part of the originator. But, it can also be a sign of fraud.

- 3) **A number of transactions that is much larger than usual.**

Again, this is something that almost never happens. But if it does, you need to contact all of the customers that received transactions and ask them if they were anticipated.

When you see such any of these three scenarios, you must act very quickly to minimize the risk of loss. A delay of more than two (2) days in reviewing and resolving unusual commercial ACH transactions will almost surely result in a loss for the bank. And trust us: the loss can be big (the largest we’ve seen is \$81,400) and your insurance won’t cover it (because it involves multiple customers and transactions).

Daily Best Practice 6—Check IATs for OFAC

Daily Best Practice 6: Check IATs for OFAC Compliance

There are up to eight fields in each IAT that must be checked for OFAC compliance:

- 1) ACH originator
- 2) ACH originating DFI
- 3) ACH recipient (your bank's customer on an incoming transaction)
- 4) Up to five foreign correspondent banks

The bugaboo here is the “foreign correspondent bank” records (aka the 718 records).

- These records are optional (less than 0.01% of IATs—that is, 1 in 10,000—have a 718 record).
- There's no way to tell if the foreign ODFI intentionally left them off, because they knew an SDN was involved in the transaction (something a large French Bank was found guilty of doing in 2014).
- However, when 718 records are present, they must be checked for OFAC compliance.
- SAM checks your IATs for OFAC compliance (including the 718 records).

Very important note #1: your bank must also be using WTM to do the OFAC checks on IATs. If you aren't using WTM, you can still print a list of names that must be check for OFAC compliance. Please see Daily Best Practice 6: Review IATs for Suspicious Activity (page 29) for more information.

5. Dashboard panel 5 (upper level, last panel on the right) has a click-through allows you to quickly check your IATs for OFAC compliance. Click on the circle and the screen below will appear.

Ofaciatfilesearch

Daily Best Practice 6—Check IATs for OFAC

6. We recommend a Tolerance level of 15 and a Last name Start position of 7.

- The first seven letters of the first name, middle name or last name must match an OFAC SDN or AKA, in order for the name from the IAT to be considered further.
 - If the first, middle or last name has less than seven letters, we must match the name exactly.
- If we pass the “Starting” test, we’ll use a comparison algorithm to determine if the letters in the IAT names match an SDN or AKA, within 15%.
 - Lowering the Starting position or raising the Tolerance level will result in more matches, all of which will likely be false-positives.
 - The most important thing to remember: the more you look at, the less you see. So, use parms that give you a reasonable amount of data to look at—and then look at it closely.

7. Review the OFAC check results.

	Name From IAT ☆	SDN Identifier	Alt-ID Identifier	SDN Name or AKA Name ☆	Type of SDN	City	Country	Tol Level Matched	Named Matched To
1	CHAN KIM	16221	24402	CHANDIO UMAR KATHIO	individual	KATIO, Muham...		100	ofac
2	CHAN KIM	9534	8956	CHANIKAN KRADOOMPORN	individual	KRADOOMPOR...		100	ofac
3	CHAN KIM	9534	8959	CHANIKAN KRADUMPHON	individual	KRADOOMPOR...		100	ofac
4	CHAN KIM	9534	8957	CHANIKAN KRADUMPORN	individual	KRADOOMPOR...		100	ofac
5	CHAN KIM	17617		KIM KWANG CHUN	individual			100	ofac
6	CHI HO CHAN	11276	11815	CHANCHIRA BOOCHUEA	individual	LIANG, Ching-f...		100	ofac

Ofactiatfilesearchscreen

- If you find a transaction being sent to an SDN, you must immediately freeze the transaction and notify OFAC.
- Please be careful; the people on the SDN list are not nice people—and the people they do business with are often nasty buggers too.
 - A few years back one of our customers was threatened at gunpoint, when they informed a customer that a large incoming IAT credit was frozen due to an OFAC violation.
 - Fortunately, no one at the bank was hurt and the customer was arrested. The customer owned a T-shirt shop and was being paid \$86,000 to produce custom shirts for a Gay Pride Parade in southern California. (Why an SDN sent him \$86,000 is anybody’s guess.)

Daily Best Practice 6—Review IATs for Suspect Activity

Daily Best Practice 6: Review IATs for Suspicious Activity

An estimated 96% of international ACH Transactions (IATs) result from on-line purchases (for example, e-bay and Alibaba. The average of these transactions is around \$9.

The other 4% of IATs are for business transactions and they can be for millions of dollars. In fact, it's not unusual for small country banks to see IATs for \$40,000 (or more). Many farmers now buy new equipment and repair-parts from China, and the transactions are funded with IATs. Likewise, small commercial fishermen on the Gulf coast are also buying equipment and repair-parts from China. And equipment used in small bars, restaurants and butcher shops often come from a few small Chinese companies that sells directly to customers and bills through PayPal. (I bought a drink cooler from a company called SPX and it is awesome!)

So, when the regulators say you need to check your IATs daily and investigate any that seem unusual, they're on solid ground. Yes ma'am and sir, most of the transactions will be small—but that means you'll spend less than one minute a day looking at them. And the once or twice a year when a big transaction hits, you'll have quick knowledge of it and can promptly confirm its authenticity with your customer.

1. Dashboard panel 8 (lower level, last panel on the right) has links to the eight most-used ACH reports. Please click on the third report (Report #8012). The screen below will appear; click Continue.

Wayne Barnett Software

Suspicious Activity Monitor

View IATs for a Specific Day

1. Date for reporting (in ccyy-mm-dd format) 2015-06-29

2. Minimum dollar-amount 0

3. Minimum number of transactions 0

4. Type of transactions to display 1. All transactions

5. Sort by 1. Account number

6. Type of accounts to include 1. All accounts

Click Continue to generate the report Continue

Click Exit to return to the previous menu Exit

latdailyselect

2. The next screen will show all accounts that received IATs for the day.

	Account Number ☆	Risk Rating ☆	Customer Name ☆	Branch Number	Excl'd Acct	High Risk	Acct Type	Tran Date	Tran Type	Number of Trans ☆	Total Amount
▶ 1	9-056-196	C 0	LOTHAR K RAUCH	7			P	2015-06-29	I-CR	1	\$226.09
2	4-048-770	C 0	KENNON D LEWIS	24			P	2015-06-29	I-DR	2	\$154.76
3	4-257-330	C 0	AUDREY A HARMON	25			P	2015-06-29	I-DR	1	\$145.04
4	229-090	C 0	JAMES R FOLSE	3			P	2015-06-29	I-DR	2	\$94.98

Daily Best Practice 6—Review IATs for Suspect Activity

latdailyselectscreen

3. If none are over \$1,000—you're done with your review.
4. However, if you have a customer who has \$1,000 or more in IATs, the regulators suggest you take a closer look at the transaction(s). Specifically:
 - i. Has the originator sent transactions to the customer before? If so, were the amounts similar and did you review the transaction then?
 - ii. If this is a "first-time transaction", is there anything about the transaction that creates suspicion?
 - Most IATs from PayPal are for small amounts, so a transaction of a \$1,000 or more from PayPal is automatically unusual.
 - PayPal will always have the name and address of the person who initiated the transaction. Sometimes, PayPal also includes notes about the transaction.
 - To review this information, click on the **Number of Trans** field and then the **Trans Date** field. This will let you review every piece of information in the IAT.
 - iii. A quick Google search on the transaction-originator may give you more confidence in the transaction legitimacy. But ... it may also make you more concerned. So please be diligent when reviewing ancillary information for IAT originators.
5. If the transaction is for \$5,000 or more, you should contact the customer and ask what the transaction for.
 - i. \$5,000 is the minimum amount for a SAR. Hence, any customer with \$5,000 or more in daily IATs should be carefully reviewed.
 - But please remember that the customer has no legal obligation to answer your questions. But if they don't answer and more transactions follow, you probably have a suspicious situation that warrants reporting.
6. If your bank is using WTM, you can automatically check the transactions for OFAC (reference "Daily Best Practice 6: Check IATs for OFAC Compliance" on page 27).
7. If your bank isn't using WTM, you can print a report of the names that you're encouraged to check, by clicking on the Print OFAC List button on this report.

Very important note #1: there is no law that requires OFAC checks. However, it is illegal to conduct business with those on the OFAC lists—and the only way to know if someone is on the list is to check their names. Accordingly, the regulators encourage you to do daily OFAC checks on IATs, but, there's no violation of law if you don't.

No ma'am and sir, the violation of law happens later, when it's discovered you did business with a prohibited person, business or country. And, banks that violate OFAC and that fail to do checks are usually fined twice as much, as those who do checks and simply screwed-up the search.

Bi-Weekly Best Practice 1—Update the CIF

Bi-Weekly Best Practice 1: Update the CIF

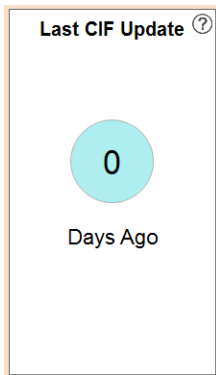
The Customer Information File (CIF) is a key part of the system. Among other things, it helps you spot ACH transactions where the transaction & account names don't match. The CIF also builds relationships (which are a key part of the risk-trigger and risk-alert processes).

The CIF should be updated prior to doing a 314(a) check. If you are also using the Wayne Barnett Systems for OFAC checks, it should be done before each of those as well.

The CIF panel on the dashboard will show a green circle, when the CIF was updated in the prior 0-14 days. It will show a yellow circle when the CIF was last updated 15-28 days ago, and red circle starting on day 29.

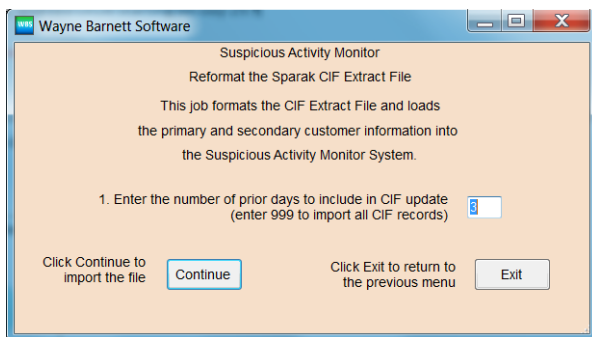
Please remember that red on the dashboard is never a good thing.

1. Dashboard panel 2 (upper level, second panel from the left) has a circle that shows the number of days since you last updated your CIF.



Ciflastupdate

2. Clicking on the circle will produce the screen shown below.



Cifimportfile

Bi-Weekly Best Practice 1—Update the CIF

3. Clicking continue will take you to a file navigation screen; navigate to the CIF file you want to import and double-click on it. The file will import and tell you the CIF update is complete.
 - The CIF update works with records that are new or recently changed. The system automatically calculates the number of prior days to include in the update.

Very important note #1: Running the CIF update in one system will result in all systems being updated.

Very important note #2: Depending on who your core vendor is, we may recommend that you always do a full CIF refresh. You can do this by entering 999 in the number of prior days. We will let you know if this process is appropriate for your bank or credit union.

Monthly Best Practice 1—Monthly IAT Review

Monthly Best Practice 1: Monthly IAT Review

We’ve already discussed the need to review IATs daily (please see “Daily Best Practice 6: Review IATs for Suspicious Activity” on page 29). There is also a need to review aggregate IATs monthly.

Why is this, you ask? Because they are international transactions—and the regulators give extra scrutiny to all international transactions.

What are you looking for, when you review monthly IATs? The answer: aggregate high dollar amounts.

What constitutes an aggregate high-dollar amount for IATs?

- We recommend \$5,000 for personal accounts (the minimum amount for a SAR).
 - We recommend \$25,000 for commercial accounts (or approximately \$5,000/week for an entire month).
1. Dashboard panel 8 (lower level, last panel on the right) has links to the eight most-used ACH reports. Please click on the fifth report (Report #8003). The screen below will appear.

iatmonthly

2. Enter the minimum dollar amount you want to check for, and, the type of accounts you want to include in your report.
 - i. As noted above, we recommend looking at all consumer accounts that have aggregate of \$5,000 or more in IATs.
 - ii. Likewise, we recommend looking at all commercial accounts that have aggregate of \$25,000 or more in IATs

Monthly Best Practice 1—Monthly IAT Review

3. Review the results.

Relating Number	CIF Number ☆	Account Number ☆	Risk Rating ☆	Customer Name	Branch Number	Excl'd Acct	High Risk	Acct Type	Tran Type	Number of Trans ☆	Total Amount
66511-102-7	66511-102-7	4-171-541	C 0	Homer Simpson	5			P	I-DR	2	\$14,257.01
				Total I-DR for relationship						2	\$14,257.01
				Total I-DR for report						2	\$14,257.01

latmonthscreen

4. Any customer on this report should be risk-rated. Likewise, you should have documentation showing what you know about the customer and the legitimacy of the IAT transactions.

- There's no law that says you must file a SAR on a personal relationship that has more than \$5,000 in IATs.
- Likewise, you don't have to file a SAR on any commercial customer that has more than \$25,000 in IATs.
- But, if you don't have supporting documentation to support your file/no-file decision, you'll likely be criticized by the regulators.

5. If you want to review specific information about an IAT on the report, please do the following.

- i. Click on the "**Number of Trans**" field to see a list of all the transactions from that originator.
- ii. Then, click on the "**Trans Date**" field to see details about each transaction.

Very important note #1: This report aggregates at the relationship level. So, if both a husband and wife have IATs and their accounts are related (that is, they sign on each other's account), inclusion on this report will be based on the relationship total. (That is, if the wife has \$3,000 in IATS and the husband has \$2,500, they will have a relationship total of \$5,500 and be included in this report.)

Monthly Best Practice 2—Monthly ACH Originator Review

Monthly Best Practice 2: Monthly ACH Originator Review

Very important note #1: This “Monthly Best Practice” is only applicable to banks that allow customers to do ACH origination.

It doesn’t matter how the customer delivers the file to the bank. (In other words, the file can be delivered directly to the bank, or indirectly via the Internet Banking System.)

Most community and regional banks do a good job of monitoring the amount of debit ACH transactions originated by their customers. However, there have been several instances where originators exceeded their limits and the ODFI did nothing to stop them. Needless to say, the regulators take a dim view of this.

To help ensure overages don’t routinely happen, the regulators have instructed the directorate to monitor their ACH debit-originators.

Very important note #2: When an ACH originator exceeds his authorized limit for debit transactions, the regulators view the overage as an unsecured extension of credit—and the overage will be classified as either special-mention, substandard or doubtful (depending on the amount).

- **Overages up to \$100,000 are usually classified special-mention.**
- **Overages of \$100,000 - \$500,000 are usually classified substandard.**
- **If your customer has exceed their origination limit by more than \$500,000, expect a doubtful classification and regulatory sanction.**

SAM gives you the ability to report the outgoing originations produced by your customers

1. Exit the Dashboard and from the Primary System Menu select options **5 > 2 > 8 Review 30, 60 and 90-day Origination Totals by Originator**. The screen below will appear.

Wayne Barnett Software
Suspicious Activity Monitor
achboardreport

Review of 30, 60 and 90-day Origination Totals by Originator

1. Ending date (CCYY-MM-DD format) 2015-11-07

2. File Type 2. Outgoing

3. Minimal amount 50,000

4. Transaction Selection Type 1. All transactions

5. Sort sequence 1. Originator ID

Click Continue to generate the report Click Exit to return to the previous menu

Monthly Best Practice 2—Monthly ACH Originator Review

Achboardreport

- Depending on the size of your bank, you'll want to set the minimum dollar amount at \$10,000 - \$100,000. (You should choose the lowest amount your bank allows for ACH originations, over a three-month period).

Very important note #3: Why do the regulators focus on amounts originated over the past three months, when the bank has to warrant consumer-ACH originations for 48 months? It's because the vast majority of disputed ACH transactions (almost 98%) are reported with 90 days.

- An example of the report is shown below.

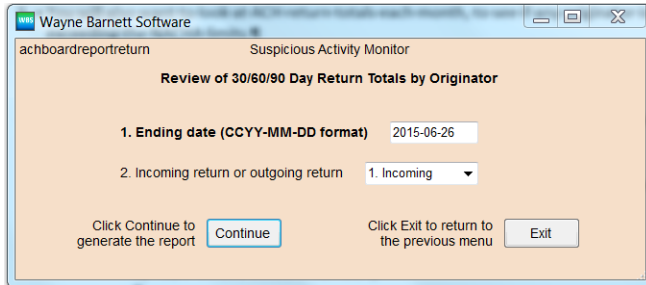
	Aggregation Period	Originator ID ☆	Originator Name	File Type	Consumer Debit Amount	Consumer Nbr of Debits	Consumer Credit Amount	Consumer Nbr of Credits	Commercial Debit Amount	Commercial Nbr of Debits	Commercial Credit Amount	Commercial Nbr of Credits
▶ 1	1 - 30 days	1010732184	Robert Sunshine	Outgoing			\$42,180.56	56			\$134,744.27	23
2	31 - 60 days	1010732184	Robert Sunshine	Outgoing			\$43,207.87	55			\$143,747.49	24
3	61 - 90 days	1010732184	Robert Sunshine	Outgoing			\$40,917.81	53			\$169,326.15	24

Achboardreportscreen

- This report shows both the credit originations and the debit originations, because the board is required to review both types of originations.
 - However, as previously noted, it's the debit originations that are of most concern.
 - You will also want to look at ACH return totals each month, to see if any originator is exceeding the NACHA limits.
 - There are three categories of returns:
 - Total returns. This is all transactions returned to the originator. NACHA rules state that returned transactions should not exceed 15% of total transactions.
 - Unauthorized returns. These are transactions that the receiver refused to honor. (There are seven return-reason codes—5, 7, 10, 29, 37, 51, 53—for unauthorized transactions.) NACHA rules state that unauthorized returns should not exceed 0.5% of total transactions.
 - Administrative returns. These are transactions returned for one of three reasons:
 - 1) R02 – Account close
 - 2) R03 – Name on transaction does not match name on account
 - 3) R04- Invalid account number
- NACHA rules state that administrative returns should not exceed 3% of total transactions.

Monthly Best Practice 2—Monthly ACH Originator Review

- To review the return totals you will have to exit the dashboard and from the Primary Menu, select options **5 > 2 > 9. Review 30/60/90 day return totals**. The screen shown below will appear.



The screenshot shows a software window titled 'Wayne Barnett Software' with a subtitle 'Suspicious Activity Monitor'. The main heading is 'Review of 30/60/90 Day Return Totals by Originator'. Below this, there are two input fields: '1. Ending date (CCYY-MM-DD format)' with the value '2015-06-26' and '2. Incoming return or outgoing return' with a dropdown menu showing '1. Incoming'. At the bottom, there are two buttons: 'Continue' and 'Exit'. The 'Continue' button is highlighted with a blue border. The window also has a standard Windows-style title bar with minimize, maximize, and close buttons.

Achboardreportreturn

Very Important Note #4: You may find it confusing that returned outgoing items come back to the bank as “incoming items-returns”, but that’s just the nature of the beast.

So, if you want to see totals for returned outgoing transactions, you want to set field #2 **Incoming return or outgoing return** to **1.Incoming**.

- Review the report and report any return rates in excess of NACHA rules to the directorate.

Monthly Best Practice 3—Monthly ACH Trigger Review

Monthly Best Practice 3: Monthly ACH Trigger Review

What the heck is a “trigger review”. That’s a great question; let us please answer it with verbiage from FinCEN’s new Customer Due Diligence Requirements (CDDR) that went into effect May 11, 2018.

“The AML program requirement for each category of covered financial institutions is being amended to explicitly include risk-based procedures for conducting ongoing customer due diligence, to include understanding the nature and purpose of customer relationships for the purpose of developing a customer risk profile.”

1. So ... what is meant by “explicit risk-based procedures” and “ongoing customer due diligence” (CDD)? Legally speaking, it means whatever you want—as long as the procedures are in writing and the regulators deem them adequate.
2. What’s the criteria for determining adequacy? That’s hard to say; there’s nothing published that addresses this. But after speaking with seven recently-examined banks, managers at two national accounting firms and 13 regulators, we’re prepared to offer our guidance on this issue. It’s outlined below.
 - i. Your customer due diligence (CDD) strategy should start by identifying customers whose recent activity is deemed significant, and therefore necessitates an in-depth review.
 - a. For ACH transactions, your monthly CDD procedure could include creating a list of all consumer customers that have \$20,000 or more in ACH transactions, and commercial customers that have \$50,000 or more. We find these amounts to be “significant amounts” for most community banks.
 - The regulators refer to these lists as “trigger lists”. All customers on the lists are there because they had significant activity.
 - The next step in the CDD procedure is to review all activity for the accounts on the lists, to determine if any “unusual activity” is present.
 - ii. In order to identify “significant unusual activity”, the bank must first determine what’s normal activity for all types of transactions, for each triggered-customer.
 - a. Your BSA system will use historical data to determine transaction-normalcy. (If you didn’t have a BSA system, your CDD procedure would take hundreds of hours.)
 - b. After a norm is established, the CDD procedure can quickly calculate a risk score, based on the customers degree of “significant unusual changes” in activity.
 - c. The import thing to remember is that large transactions don’t automatically qualify as significant and unusual.

Monthly Best Practice 3—Monthly ACH Trigger Review

- A customer with monthly incoming ACH debits of \$3,000,000 has significant but not unusual activity, if we anticipated incoming ACH debits of \$2,800,000 (a mere 7% variance).
 - But a customer with \$120,000 in incoming ACH debits, who was expected to have \$80,000 qualifies as both significant and unusual. This situation wouldn't necessarily create a BSA alert, but, it will increase the customer's risk score.
- iii. The CDD procedure for creating the trigger lists must be sufficient to reasonably identify "potentially suspicious activity".
- CDD reviews that include all transactions will typically have a review rate of 0.8 – 1.5% (or 80-150 reviews per 10,000 customers). A lesser percentage will likely be deemed unacceptable, unless bank management can provide substantial supporting documentation.
- iv. The CDD review must yield a risk score for each triggered-customer.
- a. The fact that you did a CDD review on a customer last month does not negate the need to do a new review this month, if another trigger occurs.
 - The more triggers a customer has, the greater the risk of suspicious activity.
 - b. Most BSA systems (including ours) can conduct 150 CDD reviews in 1-2 minutes. Banks without BSA software will struggle with this requirement.
- v. Your CDD review must produce a suitable number of alerts.
- a. This brings us to our final point: the "alert list".
 - A customer is placed on the "alert list" when their risk score indicates that suspicious activity may be occurring.
 - Based on what we've heard, 8 – 12% of reviewed customers should produce alerts. (In other words, 8 – 15 alerts every month, for every 10,000 customers).
 - b. Not every alert will warrant a SAR. But, every alert will require a case-file. (That is, documentation as to why/why not a SAR was filed.)
 - It's the building of the case-files that may be the most arduous part of CDDR. (Our DCK system will help immensely with this.)
 - Based on what we've heard, 10 – 15% of alerts should require a SAR.

Generate the triggers.

Monthly Best Practice 3—Monthly ACH Trigger Review

1. Dashboard panel 8 (lower level, last panel on the right) has links to the eight most-used SAM ACH reports. Please click on the seventh report (Report #7507). The screen below will appear.

Wayne Barnett Software
Suspicious Activity Monitor
achmonthlyreport

Search for Accounts with High Daily/Weekly/Monthly ACH Activity

1. ACH analysis starting date 2018-05-01
2. ACH analysis ending date 2018-05-31
3. Type of transactions 1. Incoming
4. Transactions to review 1. All transactions
5. Account types to review 3. Personal only
6. Minimum dollar amount 20,000
7. Minimum number of items 0
8. Sort preference 1. Amount

Click Continue to generate the report Continue Click Exit to return to the previous menu Exit

Achmonthlyreport

- A. We recommend you do a review of all personal accounts that had \$20,000 or more in ACH debits or credits, for the prior calendar month.
 - Why \$20,000? That's the default amount we use when calculating risk-ratings. So, if you're going to use a different amount for this review, you need to change the associated amounts in risk factors 161-166.
 - B. We recommend you do a review of all commercial accounts that had transactions totaling \$50,000 or more in ACH debits or credits.
 - Why \$50,000? That's the default amount we use when calculating risk-ratings for commercial customers that do not yet have suitable transaction baselines.
 - So, if you're going to use a different amount for this review, you need to change the associated amounts in risk factors 561-566.
 - C. We recommend that you sort the report by amount. (The reason for this will be discussed in the section below.)
 - D. Every customer on this report should be reviewed with customer due diligence (CDD); we'll cover that procedure in the section below.
2. There are three things you need to do, prior to performing CDD on your customers.
 - 1) Ensure your CIF data is up-to-date.
 - 2) Ensure all data is imported for all systems, for the period being reviewed.
 - 3) Ensure you have created baselines for all commercial customers.

Monthly Best Practice 3—Monthly ACH Trigger Review

Perform Customer Due Diligence.

When you perform CDD on all accounts on the trigger list, you'll use a series of review tools to calculate a risk rating.

1. For commercial customers, if you **ARE USING** all of our systems, the risk rating strategy looks at the 21 transaction categories we outline in the CTM Best Practice Guide. The totals for each category for the past six months are compared to each customer's baseline amounts and a risk score is derived.
 - A. The six-month period is divided into three troughs:
 - i. Prior month.
 - ii. Second and third prior months.
 - iii. Four, fifth and sixth prior months.
 - B. A positive risk finding is returned when all data in the trough (that is: data for one month, data for each of two months, or, data for each of three months) exceeds the baseline amount plus a stipulated growth percentage. (The default growth percentage is 20% and it is used by most banks.)
 - C. Each positive risk-finding adds one point to the risk score.
 - D. There is a total of 21 risk-types with three troughs per type. Accordingly, the maximum risk score from transaction activity is 63. (That is, $21 * 3 = 63$ transaction-based risk-factors.)
 - We recommend that any customer with 6 – 9 positive risk-factors be considered moderate-high risk; any customer with more than 10 positive risk-factors should be considered high-risk.
 - E. The system also has "know your customer" (KYC) risk factors. The default number of KYC risk factors is nine. Management can add-to or take-from the KYC risk factors. The KYC risk factors can lower or raise a risk scored, based on what you know about the customer.

Unfortunately, we can't answer the KYC factors for you; those you must answer yourself. However, all active KYC risk factors are automatically applied to future risk worksheets and the associated risk-rating calculations.
2. The risk-rating strategy for consumer customers is similar to the one for commercial customers.
 - A. There are 63 transaction-based risk-factors; there are as many KYC risk factors as the bank chooses to use.
 - B. The risk rating is calculated based on the customer's transactions over the past six months.
 - C. Consumer accounts don't use baseline amounts. Instead, static amounts chosen by the bank are used. The default values for the static amounts are shown below.
 - i. Cash-in and Cash-out - \$5,000


Monthly Best Practice 3—Monthly ACH Trigger Review

- ii. ACH (domestic) – \$20,000
 - iii. Wires (domestic) - \$20,000
 - iv. ACH (international) - \$5,000
 - v. Wire (international) - \$5,000
 - vi. Total debits and credits - \$50,000
- D. If you have a consumer customer that routinely has transactions greater than the amounts shown above, it's probably a commercial account disguised as a consumer account. (Loan officers often do this, so that their “good customers” aren't assessed a service charge.)

We recommend that, in the Barnett systems, you change the status of high-dollar consumer accounts to commercial accounts. This change will result in baselines being created for the customers—and that will likely result in lower risk ratings. (The risk rating will be calculated based on variance in the customer's activity, instead of variances from static amounts.)

3. For commercial customers, if you **ARE NOT USING** the CTM system, the risk rating strategy works exactly as it does for consumer accounts—but with higher default static amounts. The default static amounts for commercial customers are listed below.
- i. ACH (domestic) – \$50,000
 - ii. Wires (domestic) - \$50,000
 - iii. ACH (international) - \$10,000
 - iv. Wire (international) - \$10,000
 - v. Total debits and credits - \$100,000
4. To perform the CDD procedure (that is, to calculate the risk-rating for everyone on the trigger report), click the button in the upper right hand corner that's labeled **Risk Rate All**.

Very important note #1—Please remember that you are going to run this procedure twice (once for consumer customers and once for commercial customers).


Amounts >= \$50,000 Number of Transactions >=0									Risk Rate All	
	Routing Transit Number	Account Number *	Name from CIF record *	Account Type	Risk Rating *	In/Out	# Drs	Debit Amount	# Crs	
9	111000041	115483	FELLOWS REAL ESTATE LL...	C	C 25	incoming	5	\$80,602.38	13	
10	111000041	115649	FELLOWS REAL ESTATE LL...	C	C 25	incoming			5	
11	111000041		Total for relationship			incoming	5	\$80,602.38	18	
12	111000041	116110	JOHNS CAKE STORE CO.	C	C 3	incoming	4	\$118,070.71		

achmonthlyreportscreen

5. The most important thing from the CDD procedure is the identification of customers with a high risk-rating. But, that's not the only thing. For example:
- A. Suppose you had a consumer customer with \$48,000 in incoming ACH credits. This wasn't his only transaction for the month, but, the rest of his transactions were normal for the account type.
 - B. Our customer here has just one (1) positive risk-finding for the current month: unusual incoming ACH credits.

Monthly Best Practice 3—Monthly ACH Trigger Review

- C. The CDD procedure would not flag this account as a high-risk customer, because the customer’s total risk score is low.
 - D. And, in all honesty, his activity may not be suspicious to the bank. Large ACH transactions aren’t that unusual for small business that have a “Pay First” policy.
 - E. But here’s the deal folks: if you don’t have a reasonable explanation for the transaction, you’d need to score the customer as a risk-alert.
6. So, how do you find this customer and how do you increase his risk-rating to “risk alert” status?
- A. Step one is to review all customers based on monthly transaction-amount totals, sorted by high to low. (That’s why we suggested earlier that you sort the trigger report by amount.)
 - B. Step two: if you find a large transaction with a low risk-rating, update the rating for this customer. How do you update the risk rating, you ask? You use the bank-discretionary KYC risk factor to boost the risk-score. (In training classes, we refer to this step as “Hang a 25 on ‘em.”) The steps for doing this are outlined below.
 - i. Click on the risk-rating field for the customer. (The risk-rating field is two columns to the right of the customer’s name.)

	Routing Transit Number	Account Number *	Name from CIF record *	Account Type	Risk Rating *	In/Out	# Drs	Debit Amount
11	111000041	1135036	GLEN FOULK	P	C 0	incoming	1	\$150,000.00
12	111000041		Total for account			incoming	1	\$150,000.00

achmonthlyreportscreen2

- ii. After you click on the risk-rating field, the risk worksheet for the customer will appear. Look for the KYC risk factors that starts with the words” Bank discretionary”.

8	8	If customer is a not a borrower, customer is well-known in the community	0	NA
9	9	Bank discretionaly-customers rating warrants a higher value	25	Yes

achmonthlyreportscreen3

- iii. Change the answer for the “Bank discretionary” question to Yes; this will add 25 points to the customer’s risk score.
- iv. The customer will now have a risk-rating that will place them on the “Alerts List” for the month being reviewed.

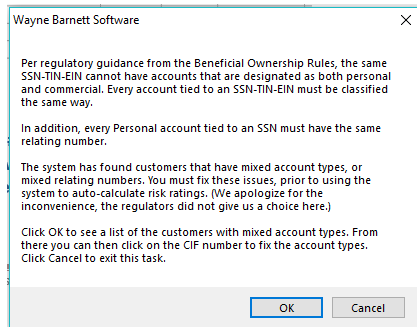
111000041	1135036	GLEN FOULK	P	C 25	incoming	1	\$150,000.00
111000041		Total for account			incoming	1	\$150,000.00

achmonthlyreportscreen4

Monthly Best Practice 3—Monthly ACH Trigger Review

Very important note #2—Please remember that risk ratings are assigned at the customer level and not at the account level. So, what does this mean? It means that all accounts with the same SSN/TIN/EIN must be classified the same way. (That is, as either personal or commercial.)

If you are performing the CDD procedure and the system finds a customer with mixed account types, the message shown below will appear and the CDD procedure will terminate.



Accounttypedifferences

If you click OK, the system will show you the SSN/TIN/EIN that has different account types.

	CIF Number ☆	Name ☆	Number of Mis-Matched Accounts ☆
1	751-632-153	ALEN ELLIOT	1
2	642-661-059	IRENE DUNCAN	1
3	466-062-308	CHAUNCEY GONZALES	3
4	465-922-112	CHAUNCEY BROWN	1
5	463-307-986	CHARLES ACKER	16
6	460-614-647	AUSTIN JUAREZ	1
7	460-596-762	AUSTIN JONES	1
8	460-417-033	FISHER QUICK STOP BEER LP	7
9	458-565-384	ALBERT HITCHCOCK	1
10	456-707-042	BECKY LUFKIN	7
11	451-349-789	AUSTIN IBANEZ	1

Accounttypedifferencesreport

If you click the number in the far-right column, you'll be shown a list of accounts that are tied to the SSN/TIN/EIN.

13		463-307-986	5-1793-7	2	C 0	CHARLES ACKER			P
14		463-307-986	5-1797-5	2	C 0	CHARLES ACKER			P
15		463-307-986	5-1898-6	2	C 0	CHARLES ACKER			P
16		463-307-986	5-1921-5	2	C 0	CHARLES ACKER			P
17		463-307-986	11-1196-9	2	C 0	CHARLES ACKER			C

Accounttypedifferencesreport2

If you click the CIF number for the account that has the different type, you'll be able to correct this error and continue with the CDD analysis.

Monthly Best Practice 3—Monthly ACH Trigger Review

The screenshot shows the 'Cash Transaction Monitor' window from Wayne Barnett Software. The title bar includes the software name and standard window controls. The main area is titled 'Update CIF Data' and contains several input fields and dropdown menus for account information. The fields are numbered 1 through 8a.

Field Number	Field Label	Value
1	Account number	1111969
2	Customer's name	CHARLES ACKER
3	CIF number	463307986
4	Relating number	0
5	Branch nbr	2
6	Exclude account from routine reporting	No
7	Designate account as a High Risk Account?	No
8	Designate account as Commercial, Personal, or Other	2. Commercial account
8a	Exempt account from mass updates?	No

Accounttypedifferencesreport3

Very important note #3—In addition to the requirement that all accounts with the same SSN/TIN/EIN have the same account type, they must also have the same relating number (if one is present.)

We have utilities to help with the account-type and relating-number cleanup tasks. Please call Wayne at 469-464-1902 and we'll help you with these chores.

Monthly Best Practice 4—Monthly Alert Report Review

Monthly Best Practice 4: Monthly Alert Report Review

The monthly review of the “Alert Report” is, in our opinion, the most cumbersome part of the new Customer Due Diligence Requirements (aka the May 11 Rules). There are basically three steps in this process.

- 1) Define what an alert is.

We recommend that your setup four risk (4) categories in CTM.

- i. Customer’s activity is as expected.
- ii. Customer’s activity is slightly unusual but not alarmingly so.
- iii. Customer’s activity is unusual, and customer is being watched.
- iv. Customer’s activity different than expected; enhanced due diligence is being performed.

	Category Number	Risk Category Description	Personal Starting Score	Personal Ending Score	Personal Accounts [☆]	Commercial Starting Score	Commercial Ending Score	Commercial Accounts [☆]
▶ 1	1	Customers activity is as expected.	-999	2	616	-999	3	551
2	2	Customers activity is slightly unusual but not alarmingly so.	3	4	146	4	6	43
3	3	Customers activity is unusual and customer is being watched.	5	6	3	7	9	13
4	4	Customers activity is different than expected; enhanced due diligence is being performed.	7	999	8	10	999	7
5		-- Accounts with no risk worksheet --			9,633			2,324

riskcategories

Any customer with a risk rating in category iii or iv should be on the alert list.

- 2) Document each alert using our Digital Customer Knowledge (DiCK) System, so that you can explain to any interested party (for example: regulators, auditors, the BSA committee or the full directorate) why a SAR was or was not filed.
- 3) Prepare a report for the directorate or its appointed committee, whereby you disclose the number of alerts, the number of new SARs filed, and the number of SARs filed for continuing activity.

Generate the alert report.

Dashboard panel 7 (lower level, second panel from the left) has a link to Report #2008, the high-risk alerts report. When you click the like, the screen below will appear.

Monthly Best Practice 4—Monthly Alert Report Review

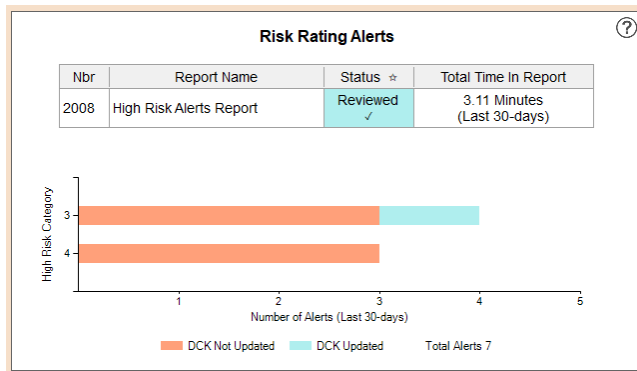
riskratingviewalerts

1. Enter the date range you wish to review and click Continue. (The default date range is the current day and 30 days prior.) The report shown below will appear.

	Relating Number	CIF Number	Nbr of Related Accounts	Risk Rating	Name	Acct Type	Risk Rating Change Date	Risk Rating Assigned By
1	465-920-203	465-920-203	2	C 5	ALBERT NORRS	P	2018-12-19	WAYNE
2		823-130-105	1	C 10	BEST VIEWS REALTY	C	2018-12-19	WAYNE
3		752-949-532	4	C 7	ALBERT ENLOW	C	2018-12-19	WAYNE
4		752-791-965	1	C 5	ALBERT ACKER	P	2018-12-19	WAYNE
5		465-821-565	9	C 8	BAKER GEARS & PULLEYS LLP	C	2018-12-19	WAYNE
6		454-724-265	6	C 10	NACHOS BOAT RENTAL	C	2018-12-19	WAYNE
7		452-447-793	8	C 8	ALBERT ALLEN	P	2018-12-19	WAYNE

riskratingviewalertsscreen

2. Every entry on this report should have an entry in DiCK, documenting why this alert is/is not being considered for a SAR.
3. The lower portion of the seventh panel on the dashboard will show the number of alerts generated in the last 30 days, and whether or not they have a recent DiCK entry. (Those with a recent DiCK entry will be represented by a blue bar; those without a recent entry will be represented by an orange bar.)



Dbpanel7

Very important note #1—For the system to register that a DiCK entry is present, the DiCK dossier must have been created or updated, subsequent to the generation of the High-Risk Alerts Report.

Monthly Best Practice 4—Monthly Alert Report Review

Very important note #2—If you are wondering what law says you have to gather supporting documentation for high risk accounts, it's 12 CFR 21.11 (which is also the law that created the Suspicious Activity Report). The regulators have cited violations of 12 CFR 21.11 multiple times over the years, when banks couldn't sufficiently explain why they didn't file a SAR on suspicious activity that came to their attention. Trust us here: if a customer is on the High-Risk Alerts Report, the regulators will conclude that their activity is sufficient for SAR consideration. So please create those DiCK dossiers.

Monthly Best Practice 5—Monthly Review of Government Benefit Payments

Monthly Best Practice 5: Monthly Review of Government Benefit Payments

Government benefit payments that are delivered via ACH are covered by federal law (instead of NACHA rules). Specifically, they're covered by 31 CFR 210.5(a), which reads as follows:

"... an ACH credit entry representing a Federal payment other than a vendor payment shall be deposited into a deposit account at a financial institution. For all payments other than vendor payments, **the account at the financial institution shall be in the name of the recipient**, except as provided in paragraph (b) of this section."

The aforementioned paragraph (b) allows for caregivers to receive benefit payments to their accounts—but only when proper documentation is filed with the paying government agency (for example, social security, railroad retirement, etc.)

What happens when one of your customers commits fraud and has his deceased mother's benefit payments deposited into his account? Well ... if he gets caught, he goes to jail and the government takes possession of everything he owns. What happens if your customer doesn't have enough money to reimburse the government? The government demands payment of the shortfall from the bank, citing the law referenced above.

In the past few years, we've spoken with dozens of banks & credit unions that found themselves in this situation. The amounts of the reimbursements ranged from \$30,000 to \$420,000, and almost of the monies were paid to the Social Security Administration.

Bottom line: banks that don't look for "government benefit payment" fraud do so at their peril. We recommend you do such a check once a month.

1. Dashboard panel 8 (lower level, last panel on the right) has links to the eight most-used ACH reports. Please click on the eighth report (#7514). The screen below will appear.

Achgovbenefitreport

Monthly Best Practice 5—Monthly Review of Government Benefit Payments

2. Enter the time period you want to review and the “tolerance level” you wish to use; the screen shown below will appear.

- A. The “tolerance level” tells the system how close the names have to be, for the system to consider it a match. We recommend a tolerance level of 50%.

Account Number ☆	Risk Rating ☆	Name from CIF Record ☆	Name from File	Beneficiary Name from Addenda Record	Originators Name	Company Entry Desc	Total Amount	Number of Trans	Tolerance
3-222-455	C 0	PEGGY M FRICKEY	JOHN SCHAUBHUT		SSI TREAS 310	XXSUPP SEC	\$733.00	1	1300%
9-112-848	C 0	HAI DUC VU	SANG M TRAN		SSA TREAS 310	XXSOC SEC	\$604.00	1	900%
4-128-916	C 0	JAY MART	WILLIAM B BLISS		SSA TREAS 310	XXSOC SEC	\$1,204.00	1	650%
595-064	C 0	JOHN F SHANKS	EDWARD J DALGA		SSA TREAS 310	XXSOC SEC	\$1,124.00	1	600%
3-127-466	C 0	D & G TRUCKING	DAVID P SAMPEY		SSA TREAS 310	XXSOC SEC	\$1,931.00	1	600%
4-199-008	C 0	BARBARA M SMITH	EDISON WOODS		SSA TREAS 310	XXSOC SEC	\$1,602.00	1	550%
635-274	C 0	DANNY B MANUEL	GEORGIE GAINES		VACP TREAS 310	XXVA BENEF	\$1,081.00	1	433%
2-521-857	C 0	SHARON M ALSAY	WAYNE J MCKINNEY		SSA TREAS 310	XXSOC SEC	\$832.00	1	350%

achgovbenefitreportscreen

3. Review the report and report any fraud you find to the proper federal agency.

- A. If a “caregiver-waiver” has been executed by the beneficiary of the payment, the issuing government agency is supposed to attach an addenda record to each ACH payment record. But, the addenda records are frequently missing.

If the person receiving the payments presents a validated caregiver-waiver for a payment, you can instruct SAM to not report the account in the future. You do this by clicking on the “Name from the CIF Record” and changing field **#12 Exempt account from ACH Gov benefits check** to **Yes**.

cifrecordupdate

Monthly Best Practice 6—Monthly Review for Crypto Currency Transactions

Monthly Best Practice 6: Monthly Review for Crypto Currency Transactions

The regulators are encouraging banks to look for customers that routinely have crypto-currency transactions.

- i. In January of 2018, a lot of customers bought bitcoins at \$18,000 each.
- ii. Four weeks later, a lot of those same customers sold their newly-purchased bitcoins for \$7,000.
- iii. If the customer was an informed consumer, his speculation into bitcoins was just bad luck.
- iv. If the customer was a novice investor, his speculative investment could have been initiated through fraudulent conveyance and a SAR may be warranted.

So, how does your bank search for bitcoin transactions? The easiest way is to search ACH transactions and look for those where the originator's name includes the words "coin", "crypto", "currency" and "byte". This function lets you do that.

1. Dashboard panel 8 (lower level, last panel on the right) has links to the eight most-used ACH reports. Please click on the sixth report (#7701). The screen below will appear.

achnamecheck


2. Click on the Keywords button to add key words to the search list.

	Keyword to Search For	Start or Anywhere	Select to Delete ★
▶ 1	coin	Anywhere in name	▼
2	crypto	Anywhere in name	▼
3	currency	Anywhere in name	▼
* 4			▼

systemparmsachname

Monthly Best Practice 6—Monthly Review for Crypto Currency Transactions

3. Please see the SAM User Guide for more information on adding key words to the search procedure. (Or, call Wayne at 469-464-1902.)
4. After you've added the key words, click exit to leave the key word list, and then click Continue to generate the report. The report shown below will appear.

	Account Number	Receiver Name	Originator Name	Keyword Matched	Originator ID	Originating DFI	Amount	Processing Date	SEC Code	Tran Code	Tran Type
▶ 1	1138410	GREENE RESTAURANT CO.	COINBASE.COM/B	COIN	1455293997	02121486	1,002.97	2018-05-17	PPD	22	Cr
2	1138410	GREENE RESTAURANT CO.	COINBASE.COM/B	COIN	1455293997	02121486	2,564.30	2018-05-07	PPD	22	Cr

achnamecheckscreen

Very important note #1: you can also use this function to search for other transaction key words. For example, you may want to search for such key words as “ISO” (may indicate the company is settling private ATM transactions, “CASINO” (may indicate a tribal casino that is settling cashed checks through ACH) and others.

Quarterly Best Practice 1—Risk Rating Cleanup

Quarterly Best Practice 1: Risk Rating Cleanup

When a risk-analysis is performed on a customer, a risk-review date is automatically assigned by the system.

In the days prior to CDDR (aka the May 11 rules), it was normal to update risk ratings every 3 – 12 months, depending on the risk score. Well ma’am and sir, that’s changed. These days, many of your customers will have new risk ratings every month—even if they’re low risk.

Why is this? It’s because the customers will routinely show-up on the trigger reports (please reference “Monthly Best Practice 3: Monthly ACH Trigger Review” on page **Error! Bookmark not defined.**) The trigger reports will let you show the regulators that you’ve identified everyone with significant transaction activity. The risk-rating will show the degree to which that significant activity is deemed unusual.

But, what do you do with customers that had a trigger 12+ months ago, and nothing since? We recommend you archive these risk rating—and that’s what we’ll show you here.

1. Exit the dashboard and select options
 - Click Admin functions (option 10)
 - Work with databases (option 3)
 - Work with Risk Rating database (option 4)
 - Archive risk rating worksheets (option 1)
 - Archive low-risk rated worksheets (option 2)

riskratingarchivelowriskutility

2. Click Continue to archive risk ratings that are low-risk and no longer deemed relevant.

Very Important Note 1: This system function will automatically archive any risk rating that meets two tests:

- i. **The last risk rating was done at least three months ago.**
- ii. **The current (updated) risk rating is a low-risk score.**

Quarterly Best Practice 1—Risk Rating Cleanup

You must manually archive any risk rating that doesn't meet these two criteria. Please reference the SAM User Guide for instruction on archiving risk ratings. Or, call Wayne at 469-464-1902—he's always happy to hear from folks.

Thank you for using Wayne Barnett Software

Thank you for being our customer, we appreciate you. If you have any questions about this guide, or, ideas for improvements, please let us know.

wbarnett@barnettsoftware.com

469-464-1902