

AML Services International, LLC

Transaction Monitoring: Using Statistics to Create Peer Groups and Reduce False Positives

By Saskia Rietbroek, CAMS
October 2008

Special thanks to Erik Middelkoop from IEQ Netherlands for his contributions to this article.

Monitoring customers purely on the basis of historical activity can be misleading if their activity is not actually consistent with similar types of customers. Sometimes you need more advanced detection capabilities to detect true unusual behavior and reduce false positives. One way of doing this is to create peer groups. What is peer group analysis, you ask? Read on to learn more about this method, what the regulators expect from financial institutions and how to create reliable peer groups using statistics.

Peer group analysis is a methodology that is not only based on what is reasonable and expected for a customer's historical activity, but also uses a comparison of that customer to similar customers. For example, restaurants with the same annual turnover, or individuals with the same age or living in the same postal address, county or zip code would be compared to each other.

For instance, if I write checks totaling \$1,000,000 per month that would be unusual for me. However, if Bill Gates does that, it is not out of the ordinary. It might also be normal if Gates's neighbor writes \$1,000,000 in checks per month. They probably both live in a nice area somewhere in Silicon Valley. If you were working with software using a detection scenario that just uses a dollar threshold of \$10,000 in checks per month, Bill Gates and his neighbor would get an unnecessary alert. By creating peer groups you can avoid these false positives.

You want to avoid comparing my more average income behavior with that of one of the richest men in the country. The best way is to set up peer groups, and compare my behavior with the behavior of my neighbor, and Bill Gates behavior with that of his neighbor.

Or, to give a business example: If your transaction monitoring software is using detection scenarios that look at businesses and you have set only one threshold for the cash behavior of all of your business customers, you will probably get false positives, because what is normal for a large supermarket chain, is not normal for a small grocery store. It makes more sense to analyze the behavior of an account not only historically, within its own account, but also across peer groups - similar restaurants with the same sales volume, for instance.

Use deeper analysis to detect true unusual behavior

Peer group analysis is effective at discovering suspicious transactions by first comparing every transaction against its corresponding account history to determine if the behavior is unusual. It then, for further analysis, compares the activity against a relevant peer group which is, perhaps, industry specific or customer type based. So the alert

AML Services International, LLC

generation process will not only look at whether a certain dollar threshold has been met, and whether there is a spike in activity for this account, but also compares the behavior with other members of the same peer group.

For *retail* customers, which peer groups would you most likely use for purposes of detecting financial crime? Age, Zip/postal code, or profession? At first glance, you might think profession - but be careful, professions change. Someone is a student today and a doctor tomorrow. It is better to use "hard" data that you have in the financial institution, such as date of birth or zip code.

Peer group analysis greatly reduces the false positives and provides a better understanding of what is really unusual and an actual risk. Typically we look at the behavior of the account itself over time. We monitor transaction volumes and frequency across a span of time. For example, if a customer made two deposits monthly for a set amount into an account over a year period and then suddenly makes a third deposit one month for a different amount, this could appear to be unusual, according to the account history. But when compared to a peer group, that transaction turns out not to be so suspicious. On the flip side, the peer group analysis can also discover risks that an account history review would not.

Examples outline value of peer group analysis

Let's give another example: You can get an alert because you have a detection scenario that just looks at whether a dollar threshold was met. For example, an alert is triggered when someone deposits \$10,000 in cash. Is this a useful alert? Not really. This could be normal behavior for this customer. You need to know more about the customer to be able to qualify the alert and see if it merits a suspicious activity report, or SAR. The alert could be a false positive...

What would happen if we actually used a peer group based on the age of the customer? There was a deposit of \$10,000 in cash, and the customer is 12 years old. Can you use age for setting up peer groups? Yes, you can. This is information you typically have on file. In many countries as part of your customer identification program you need to capture the date of birth, so that information is in your bank, insurance company or credit union. Now, the alert has become more interesting because it is not typical for a 12-year old to deposit \$10,000 in cash.

With peer group analysis, an account set up for the specific purpose of money laundering can readily stand out because the account deviates from what the accounts its peers would show when profiled against their peer group.

One more example: A business account of a pizzeria is set up for money laundering. The pizza parlor seemed to have consistently high sales throughout the year with no lows or specifically very busy periods. A review of just the account activity would not reveal suspicious activity because the deposits were consistent. The account has always shown this behavior. However, by comparing the activity with other pizza restaurants, the account suddenly appears very suspicious because similar restaurants tend to experience a dip in sales after the Christmas holiday and the profiled pizzeria did not.

AML Services International, LLC

Similar types of industry specific comparisons can unveil suspicious behavior that you otherwise would not detect.

So the 'Peer Group Comparison' function allows real customer data to be used as a benchmark for average or "normal" activity. Activity which is outside a pre-defined span of this benchmark is then sent to the equivalent of an exceptions queue for investigation, or triggers an alert.

Regulators expect more out of transaction monitoring

The regulatory compliance landscape is getting increasingly tougher. The International Standards on Monitoring, Screening and Searching Statement, issued by the Wolfsberg Group a few years ago, mentions the importance of creating peer groups in transaction monitoring efforts. In this statement, the group says, in the section on "Standards for Risk-Based Transaction Monitoring," that "An effective risk-based transaction monitoring process should compare the client's account/transaction history to the client's specific profile information and a relevant peer group and/or compare the clients account/transaction history against established money laundering criteria/scenarios, in order to identify patterns of suspicious activity or anomalies."

The regulatory compliance landscape in the U.S. is also getting increasingly tougher. The FFIEC Manual says, "Monitoring customers purely on the basis of historical activity can be misleading if their activity is not actually consistent with similar types of customers. For example, a customer may have a historical transaction activity that is substantially different from what would normally be expected from that type of customer (e.g., a check-cashing business that deposits large sums of currency versus withdrawing currency to fund the cashing of checks)."

Save time and money with fewer false positives

Now, let's look at the other reason why you should be thinking about using peer group analysis in your monitoring efforts. Alerts must be investigated by AML professionals, but in many occasions they "waste" a lot of time, and thus money, on false positive alerts, i.e. the wrongly flagged alerts. AML solutions can be extremely inefficient in the sense that they generate a lot of false positives.

This inefficiency has a negative impact on a bank's, or other financial institution's, return on its investment. Managing false positives is a large part of the operational costs of the AML system itself. Many of these alerts turn out to be false positives. But you can't simply delete an alert. You need to document why you believe it does not merit a case, suspicious activity report or further investigation, and that takes time... and money. Therefore, productivity and efficiency increases related to alert triggering and investigation management is a key cost-savings factor.

Statistics 101: Mean, standard deviation and z-scores

To best take advantage of this, thorough identification and selection of peer groups is the main skill required. Not all peer groups will work well. The use of statistics is

AML Services International, LLC

extremely important. What we want to do is detect unusual behavior. But in reality you don't know what is normal and what is not.

If you have a detection scenario that selects accounts with a turnover of more than \$10,000 in cash in one month, that is not very useful because it may be normal behavior for many people. And thus create a lot of false positives. That is why you make an extra filter that uses the same detection scenario, but that deletes all the alerts for the accounts for which \$10,000 in cash deposits in one month is normal behavior, and just gives you the alerts for the accounts where this is not normal.

Let's assume you use the detection scenario that we just discussed and 100 accounts retail customers meet the threshold of > \$10,000 in cash in one month, and would generate an alert. Maybe you will have 98 false positives. But in those 100 alerts there were actually two useful alerts. One is an alert of a child of 12 years old who made the deposit, and the other of a 33-year-old customer who has been unemployed for six years. So, if we agree that for these two the \$10,000 was unusual behavior, then, how do we achieve to get just these two alert, and not the other 98?

We do that by segmenting the clients by peer group and the statistical values that we need to determine the reliability of a peer group to see if an alert should be generated. These include the following: Mean, STD and z-score.

First, we need to calculate the average or mean of the cash behavior of a peer group because we want to know what is NORMAL for this group in terms of cash deposits. We want more accurate alerts, to get rid of false positives, but we also want to keep that alert of the 12 year old who made the 10,000 cash deposit.

Next we look at the standard deviation, or STD. It measures how widely spread values in a data set are. If many data points are close to the mean, or average, then the STD is small; if many data points are far from the mean, then the STD is large. What we mean by that is the peer group cannot have a behavior that is all over the place; that is too wild. If the STD is too large, a peer group is not reliable.

For example, if you want to set up a peer group for check behavior, and it turns out that the members of the group use checks for buying groceries (small amounts), but also when paying a down payment for a house (big amount), the peer group won't work. The values or data points will be too widely spread, and the STD too large.

The last statistical value that we need in the peer group analysis is the z-score. This is the number of STDs from the mean. If the z-score is very high, for example, if it is more than 10 STDs from the mean, the individual's behavior is extreme for the peer group that he or she is a member of. And thus an alert should be generated.

Putting it all together

You can use Excel® to do all the necessary calculations for the different peer groups, and you can verify whether the groups pass certain reliability thresholds, such as:

AML Services International, LLC

1. The groups must have enough members. If you only have a couple of members, the group is not reliable enough to be able to establish normal behavior.
2. Standard deviation cannot be too large. The behavior cannot be too wide spread in a group.
3. Use z-score to qualify alert. If the z-score is high, then the behavior is extreme and an alert must be generated.

All of this is then used in the detection scenarios and a decision is made whether to create an alert or not.

It is best to use peer groups as additional “qualifiers” for alert generation in detection scenarios with low thresholds. These detection scenarios can potentially create a lot of false positives, and thus we can make it better by using peer groups to quality the alerts before sending them to the AML analysts desktop.

Four steps to more efficient suspicious activity detection

So here are the steps:

1. Determine appropriate peer groups. Again, you need to find groups that might show similar behavior. Same age in the same zip code, for example. Or certain size businesses in the same line of business.
2. Establish reliability of a small group, so the STD cannot be too large, but there must be enough members in the group for the peer group analysis to be used. If reliable, calculate z-score, and if the z-score is very high, then you generate the alert. If the z-score is too low, delete the alert.
3. If the group is not reliable, the system will calculate reliability of large group (ideally an account is part of more than one peer group). If reliable, calculate Z-score and determine based on the peer group whether the alert is good or not. If the Z-score is high, then the behavior is extreme and an alert should be generated.
4. If both groups are not reliable, the alert will be generated *without* using the peer group. This is just to stay on the safe side. You might want to send these “raw” alerts to a specific workflow because they are more likely to be false positives.

As you can see much can be missed by just using simple thresholds in your transaction monitoring. By following these steps and guidelines you too can use statistics and peer group analysis to strengthen your transaction monitoring program. Not only will you meet the growing demands of regulators, but you will do so by saving time and money.

Saskia Rietbroek, CAMS, is the founding Executive Director of the Association of Certified Anti-Money Laundering Specialists (ACAMS), and a member of the ACAMS Advisory Board. She is partner in AML Services International, a risk and compliance consultancy (www.nomoneylaundering.com). She is also Financial Crime Advisor to Fiserv Fraud and Compliance, a leading company in financial crime detection. She can be reached at saskia@nomoneylaundering.com.

2008 © AML Services International, LLC

Tel. +1-305-608-7888

www.nomoneylaundering.com

saskia@nomoneylaundering.com