



## CASE STUDIES

### Examples of analytical experiences detecting fraud and abuse with RiskTracker™ Account Activity Analysis System

*The following are descriptions of actual situations encountered by BANKDetect's client banks in their efforts to prevent losses using the RiskTracker™. Only Case 1 is attributable as it was a published article in Security Management Magazine. The remaining cases are not attributable to protect client privacy.*

---

#### **Case 1**

*Article by Kevin Null, Chief Security Officer, Provident Bank, Security Management Magazine*

“Each bank must decide for itself what its criteria will be for flagging suspicious transactions. At Provident Bank, the criteria have evolved as the fraudulent activity has changed. For example, when transaction reports were first implemented a few years ago, a transaction was flagged if it involved an account that was between 30 and 90 days old that suddenly exceeded its average daily balance by a certain percentage because a check in the amount of \$5,000 or more was deposited. As suspects realized that their checks were being flagged and accounts frozen, they began lowering the amount of each fraudulent check to get under the bank's threshold. Security has consistently lowered that threshold; today, check deposits of \$1,000 or greater made into new accounts are included in the transaction report.

When an item is flagged, bank security checks the history of the account to see whether further investigation is warranted. For example, security will check whether previous deposits have cleared. If a transaction still seems suspicious, security will obtain a copy of the suspicious check and call the other financial institution to verify funds.

In 1996, the first year of the program, Provident Bank avoided \$667,277 in potential losses by identifying deposited items that would have been returned as nonsufficient funds, account closed, or counterfeit.

However, because the bank has lowered the threshold amount, the number of transactions that appear on the report has grown substantially, making it difficult, if not impossible, for security personnel to review all items. The bank has since purchased a

software program that will filter activity based on criteria that security specifies, such as the age of the account, the amount of the deposit, and the average daily balance. The software, called Risk Tracker by BANKDetect of Churchton, Maryland, is integrated with the bank's account processing program and checks all bank transactions. The system then prioritizes and rates the risks. In 1998, it helped the bank identify and prevent \$1.4 million in potential losses.”

---

---

## **Case 2**

A customer of a Washington, DC area bank operated a business checking account for approximately six months before beginning to receive frequent large cash deposits. Deposits over a one week period reached nearly \$150,000. The account was a business account, with the reported business being telephone charge card sales. However, the address of the account was the individual's home address. The telephone cited for the account was determined to be a cell phone.

After the initial cash deposits, wires were used to send several large transfers to banks in the area of Detroit, Michigan – a location with high crime and a population with potential overseas and possibly terrorist connections.

On occasion, wires from Detroit banks were received in the Washington account. The RiskTracker™ detected the cash deposits immediately, as well as the unusual change in activity from the prior low level of activity during the account's initial six months. The outgoing and incoming wires were highlighted as suspicious and the RiskTracker™ produced a high risk score for the account.

On review by the bank, it was determined that the business operation was suspicious – *it would be implausible to expect \$150,000 in cash sales of telephone cards in one week from a home operated business. Any sales of such magnitude would likely be to corporate customers who would pay by check or other non-autonomous means.*

The bank filed all appropriate cash transaction and suspicious activity reports, then closed the account because of its unusual behavior and risk.

---

---

## **Case 3**

In an east coast bank, RiskTracker™ detected periodic checks being deposited to a personal account for the exact amount of \$9,000. The frequency of the deposits was at two week intervals. Since the account was relatively new (i.e., less than 60 days old) the RiskTracker™ highlighted the checks as being unusual deposits on the basis of their suspicious amount, the contrast with prior account behavior, and the duplication of the amounts.

On examination by bank analysts, the check numbers were found to be nearly sequential, even though they were issued at two week intervals. This was considered suspicious because the company on which the checks were drawn was a large real estate management firm that typically wrote nearly a thousand checks per week. The company had an account with BANKDetect's client bank, as well as with another bank, where the drawing account was located.

Further examination of the personal account showed that the individual had another account with the client bank. That account showed a series of similar deposits going back for over two and one half years.

The bank's analyst contacted the company to suggest a review of the checks in question. The company initially indicated that everything must be in order or they would know of the problem. However, after briefly looking into the checks, the company requested the bank's assistance in a closer examination of the suspicious history of both personal accounts. The examination revealed that a bookkeeper for the company had been embezzling funds for nearly three years. The total amount of the loss to the company was \$1.8 million.

Although there was no associated loss to the bank as a result of this case, the good will that was established with a major bank customer was invaluable and became a major asset to the bank's relationship with this and other corporate customers.

---

#### **Case 4**

Two of BANKDetect's client banks held business accounts with the same company. Large amounts of deposits and withdrawals were made between the two banks and with a third large bank. The RiskTracker™ repeatedly identified the deposits as unusual in amount and as variations from prior behavior because they were consistently increasing over time. They were also suspicious as they represented a pattern of transactions between the same three banks. Each of the suspicious transactions was maintained in RiskTracker's™ history and was used as part of both the automated and manual analysis. Because, U.S. banks frequently grant availability of deposited funds before they have actually been collected, the amount of the exposure to the banks was also increasing.

Analysts from one of the BANKDetect client banks reviewed the account and determined that there was a high risk of check kiting. At that point, approximately \$370,000 was at risk if outstanding checks were returned unpaid. The bank closed the account and called the second BANKDetect client bank to make sure they had detected the problem account also. RiskTracker™ had accurately detected the risk at the second bank and the account was closed there also. As a result of their actions, both banks were able to prevent the losses that were associated with this account – which were passed on to the third bank as it continued to keep the account in operation.

---

---

**Case 5**

At a Midwestern bank, RiskTracker™ detected a series of unusual transactions in a small business account that had been opened for approximately three months. Analysis detected a series of cash deposits that were always below the minimum reporting threshold of \$10,000. RiskTracker™ automatically detected the individual cash transactions, but it also was able to detect multiple deposits at several branches of the bank during the same day. This fired indicators for “Multiple branch” activity as well as for “Multiple deposits.” The analysis automatically determines if the amounts of multiple deposits aggregate to a “breakpoint cluster,” or evidence of attempts to manipulate the transactions so they do not trigger cash transaction reports.

Because RiskTracker™ highlighted the account, bank analysts continued to monitor its activity. As balance grew to approximately \$150,000 RiskTracker™ detected three wires of \$25,000, \$60,000 and \$60,000 to another U.S. bank. Within a week a wire into the account was received for \$50,000.

As soon as the wire in was received, there was a rapid increase in ATM withdrawal activity across the city. Maximum withdrawals were made to the account for as many times a day as was permitted until the balance of the account was drawn down to about \$1,000.

Upon initial investigation and reporting the activity to law enforcement it was determined that the account holders were part of a mobile gang that was moving across the country conducting fraud, robberies, and weapons sales. Typically the gang would open accounts at local banks prior to beginning operations. They used counterfeit corporate documentation and false identities to open the accounts. They usually remained in operation for a couple of months and then moved on. The wires in were estimated to be for the purchase of drugs and for other expenses in preparation for moving to another location.

The bank closed the account and subsequently law enforcement apprehended several of the gang members.

---

---

**Case 6**

On an established small business account in a mid Atlantic bank, RiskTracker™ detected a significant increase in the number of checks being cashed over the counter. The indicators fired were “Activity change,” “Multiple withdrawals,” “Multiple branches,” “Check numbers out of sequence/range,” and “Suspicious amounts.” The combination of indicators alerted bank analysts to unusual activity on the first day of a stolen check scam. Although \$2,500 had been cashed at the teller line the rapid detection by

RiskTracker™ permitted bank analysts to contact the client company and determine that the checks had not been issued and had been stolen.

A new cleaning crew had been hired by the company and had gained access to the accounting offices, stealing checks from the bottom of a drawer. Although the criminals were not apprehended, RiskTracker's™ rapid detection of the problem permitted the losses to be stopped before a second day of withdrawals could be made.

---

---

### **Case 7**

In a southern U.S. bank, RiskTracker™ detected two cashier's check deposits for \$8,500 each at two branches in the same day that totaled \$19,000. The checks were deposited to a recently opened account(52 days earlier). Until these transactions the account had maintained an average balance of \$135 and had been used only slightly with about 4 transactions per month.

RiskTracker™ analyzed these transactions and concluded the following RiskIndicators: "New account," "Low average balance," "Low activity," "Activity change," "Suspicious amount," and "Duplicate amounts." Even though these checks were "official" checks that would not normally indicate collection risk, the analysis nevertheless highlighted them as being unusual for the account's prior activity.

On examination, the checks were determined to have been "washed" and the amounts doctored. Investigation showed that the deposits had been made by criminals who had purchased cashiers checks at another bank for \$25 each, specifically intending to use them in the scam.

---

---

### **Case 8**

A client bank installed a number of shopping mall branches and ATMs. Since these outlets were available for extended hours, including weekends they became favorite targets for various scams. For example, ATM "deposits" were made using empty deposit envelopes but claiming amounts of several hundred dollars. Bank policy was to extend \$100 automatic credit to such transactions. Over the weekend, fraud criminals would make multiple false deposits followed by \$100 withdrawals at as many different outlets as possible.

Although the bank did not want to revise their credit policy for ATM deposits, they wanted to be able to detect and track these transactions so that they could rapidly take action on the accounts. The RiskTracker™ was modified to permit it to selectively identify ATM transactions made at high risk locations and analyze the transactions in context with account history. Since the vast majority of the fraudulent accounts were

opened only for the purpose of conducting these scams, they were relatively easy to identify because they lacked the usual history of a normal account.

Although money was lost, the bank was able to close accounts and report enough of the activity to law enforcement that the scam activity was reduced to an acceptable low level.

---

---

**Case 9**

At a Midwestern bank, fraud criminals began a scam that included opening two new accounts under common ownership. The scam involved seasoning both accounts for several months until they became normal looking. Then one or more large deposits were made to one of the accounts using counterfeit cashier's checks or money orders.

Funds for the "official" checks were immediately made available to the account. On the day after the deposit, a telephone transfer request would be made to move a substantial part of the initial deposit to the other account where it was rapidly withdrawn. The internal transfer was used as a method of removing any question of fund availability and also made the tracking problem more complex.

Upon the client bank's request, BANKDetect developed a new detection module for this scam and incorporated it into the RiskTracker™. The new module combined tracking of relatively new account transactions with detection of suspicious deposit amounts and activity changes. In addition the telephone transfer request was added as a transaction type that is tracked by the system. Combining all of these RiskIndicators with the proper parameters and weights gave the bank the ability to rapidly detect the scam and place prevention measures into action.

---

---

**Case 10**

A number of domestic and international gangs have consistently attempted to place gang members or representatives into employment at banks across the country. The "plants" are used for a variety of purposes – typically to embezzle money from the bank by moving funds internally, and to steal account detail documentation.

A client bank was faced with the above problem and requested BANKDetect's assistance in tracking employee accounts as one method of detecting unusual transaction activity. The solution was simple. BANKDetect created an "Employee Region" within the RiskTracker™. All employee account transactions were passed to this internal "region" for analysis. Because regions within RiskTracker™ can be set with unique parameters and therefore permit different analysis to be performed, the employee accounts could then be subjected to special analysis.

Although no new analysis modules were needed to accommodate this solution, the existing modules were set up to be more sensitive to unusual changes in account activity and other suspicious transactions. This method of internally monitoring employee accounts has been highly successful and is currently employed by most BANKDetect clients.

---

**Case 11**

In a southern bank there were two unusual problems to solve. The customers of the bank included a large number of older individuals who moved from the north to the south during winter months, returning north for the summer. Many of these “snowbird” customers were wealthy and maintained unusually large balances in their checking accounts. Some of these same accounts were also “sweep” accounts used for daily investment of available funds.

The problem was that snowbird accounts would lie relatively dormant for part of the year and suddenly experience a large deposit transfer and increase in activity. Because sudden changes in account behavior are frequently an important indicator of fraud, the RiskTracker™ would highlight these accounts as high risk – when in fact they were high value customer accounts.

This problem was further complicated when the sweep accounts were added. Although the actual balance of these accounts could be several million dollars, after the nightly sweep was performed the apparent available balance was almost zero.

To prevent the bank from experiencing false positive hits on these accounts and their associated transactions, BANKDetect developed sophisticated analysis logic that has the ability to accurately identify both of these situations. Changes to the snowbird accounts were typically in spring and fall and this was used as one method of moderating the impact of sudden changes. When combined with the age of the account and average balance calculated over a longer period, it was possible to identify these accounts.

The sweep accounts were identified by intelligence incorporated in the account number which permitted these accounts to be identified and analyzed separately from other accounts.

Both of these solutions were incorporated into the baseline RiskTracker™ system for potential use by all clients.