Attain Insight

Turning ATM Transaction Data into Fraud Intelligence: How Map Intelligence from Attain Insight reveals patterns of fraud across locations and time

Fraud teams spend much of their time looking for signs that something is wrong. A suspicious card number. A deposit amount that doesn't match. A withdrawal that follows a deposit too quickly.

For one Canadian co-operative bank, the bigger challenge was fitting those clues together into a broader picture. While each clue matters, each one only tells part of the story. Is a suspicious ATM transaction an isolated event? Or is it one point in a wider pattern moving across several machines, locations, and days?

Attain Insight helped the bank bring that larger picture into focus. Using Map Intelligence within IBM Cognos Analytics, the bank's fraud team can now analyze ATM activity geographically, giving investigators a faster way to identify patterns, investigate suspicious activity, and understand whether individual incidents point to a broader fraud problem.

Connecting Fraud Clues Across the ATM Network

The bank regularly uses its established processes for identifying potential ATM fraud. Its teams can review balance reports, investigate individual records, and compare ATM totals against the amounts entered at the terminal. These methods can reveal important anomalies.

But record-level analysis has limits. It can help close a case, but it doesn't always help the fraud team see whether similar activity is occurring across multiple ATMs, whether the activity is geographically concentrated, or whether events might be connected.

That distinction matters because ATM fraud often has a geographic dimension. Fraud can concentrate around specific machines or hot spots, shift from one area to another, or involve activity that looks anomalous when compared with a cardholder's usual location patterns. Those relationships can be difficult to detect in rows of records, traditional reports, or daily reconciliation processes. But with a location-aware view, those connections are easier to see.

Why Location and Time Change the Investigation

ATM fraud isn't just a transaction problem. It's also a location and time problem.

Traditional reports can show card numbers, deposit amounts, withdrawal activity, and exceptions that need follow-up. But they don't always show how suspicious activity moves across a network of ATMs. A card that was normally used in one place may suddenly appear somewhere else. Activity that looks like a series of separate events in a report may look different when it's viewed across machines, locations, and days.

In a simple deposit fraud scenario, the team may be trying to understand whether an ATM total matches what was entered at the terminal.

In a more complex case, the team may be looking for large deposits and withdrawals, activity outside a cardholder's normal geographic area, or transactions that suggest a compromised account.

By putting ATM activity on a map, the bank could begin to visualize not just what happened, but where it happened, when it changed, and whether individual events were part of a larger fraud problem.

Bringing Map Intelligence into the Cognos Workflow

Attain Insight helped the bank bring that location-aware view directly into its IBM Cognos Analytics environment with Map Intelligence. Rather than requiring fraud analysts to work in a separate mapping platform, the solution made geographic analysis part of the reporting experience the bank already used.

In practical terms, Map Intelligence gave the fraud team a new way to visualize ATM activity. The solution enables analysts to view suspicious activity on a map and analyze it by location, card number, transaction type, time period, deposit and withdrawal behaviour, and other fraud indicators.

Attain Insight configured the reports, filters, thresholds, and map views around fraud indicators specific to the team's work. Analysts needed to look up a card number, see where it had been used, and compare activity by day or week. They also needed to quickly identify changes in transaction volumes, deposit amounts, withdrawal patterns, and activity that happened outside a cardholder's normal geography or across several ATMs.

The first goal was to help the fraud team handle familiar issues, such as deposit discrepancies and suspicious card activity, more efficiently. From there, the work expanded to include more complex patterns, such as unusual deposits and withdrawals that might indicate a compromised account or potential money-laundering activity.

For the bank's Cognos users, the experience was a natural extension of the existing analytics

environment. A map could function like another reporting object, giving the fraud team a more visual way to work with trusted data and investigate suspicious activity without replacing its processes.

Seeing Where Suspicious Activity Starts, Stops, and Spreads

With the new geospatial views, a known card number can be reviewed across a defined period of time to show where it was used, when activity started, when it stopped, and whether it remained around one ATM or spread across several machines. If a cardholder's normal activity was concentrated in one area but new transactions appeared somewhere else, the team could see that geographic shift more clearly. The result was a more practical investigative view: location, time, transaction type, and card activity in one place.

That changed the investigation from a record-by-record review into a more complete view of activity across the ATM network.

Investigating Faster and Strengthening Fraud Intelligence

The most immediate benefit was speed. With Map Intelligence, the fraud team could get to the information it needed much faster when investigating basic ATM fraud issues.

That speed matters because ATM fraud investigation is often a race against continued exposure. If a bad card is identified and reported more quickly, the originating institution can shut it down sooner. That can reduce the chance that the same card will continue to be used across the bank's ATM network.

The bank also gained a clearer view of whether suspicious activity extended beyond a single case. Instead of closing individual investigations in isolation, the fraud team could look across machines, locations, and time periods to see whether related activity was occurring elsewhere. That helped the team move closer to proactive fraud intelligence, where the goal is not only to explain what happened but to understand whether it points to something larger.

In addition, being able to identify and report suspicious activity more effectively strengthens risk management and provides better support for fraud reporting.

As the bank continues to refine its fraud reporting, the same intelligence can be leveraged in IBM Planning Analytics to forecast fraud activity, identify emerging risk areas, optimize investigative and security resources, and evaluate potential mitigation strategies. By combining location intelligence, fraud analytics, and planning, the bank can move beyond understanding where fraud has occurred to proactively model future risk and determine the most effective operational response.

From Isolated Clues to Actionable Patterns

For the bank's fraud team, the value of Map Intelligence was being able to ask high-impact questions: does this event stand alone, or does it point to a broader problem?

That question is difficult to answer from individual records alone. By extending IBM Cognos Analytics with Map Intelligence, Attain Insight gave the bank a way to bring transaction activity, location, and time into the same investigative view. The result is a stronger way to follow the clues, see patterns earlier, and decide where the investigation should go next.

Map Intelligence for IBM Cognos Analytics™

Map Intelligence expands the native mapping capabilities of IBM Cognos Analytics to bring more spatial data, richer interactive maps, and advanced spatial analysis to dashboards and reports.

LEARN MORE

attaininsight.com
info@attaininsight.com
+1 (833) 235-0200
+1 (613) 235-0200