TigerGraph

Solution Brief

A Data-driven Approach to Intelligently Detecting and Disrupting Illicit Activity by the World's Top Financial Institutions

Better Approaches to Fighting Financial Crime

Online fraud will cost businesses more than US $200 billion between 2021 and 2024 according to Juniper Research. Fortunately banks have a powerful weapon in the war against fraud: graph analytics combined with artificial intelligence. Together these powerful technologies can uncover suspicious financial patterns in ways that other approaches cannot—helping to stop crime before it can be committed. It's no surprise, then, that banks are investing in graph analytics.

Graph and AI can analyze thousands of customer data points—and the crucial relationships between them—to deliver fraud alert scores in real time. Graph can be used for fighting financial crime by analyzing the links between people, phones, and bank accounts (among other things) to reveal indicators of fraudulent behavior, not only helping banks pinpoint suspicious activity in a sea of data but also giving them the tools to explain what's going on.

A key feature of graph is its ability to perform at speed, especially compared to relational database solutions such as SQL. Banks have been doing fraud detection for years, but one of the things that graph brings to the party—apart from depth of analysis—is speed. While SQL depends on bulky table joins, graph is less memory intensive and able to handle a greater query load.

Graph analytics provides financial institutions with the ability to:

- **Detect financial crime better.** By leveraging analytics on a global scale, banks can more accurately identify patterns and potential criminal activity and broader networks that might not be possible with existing technology.
- **Investigate suspicious activity quicker.** Graph analytics gives investigators detailed insight of criminal behavior. Financial Institutions have the ability to more quickly and accurately make connections and build comprehensive global networks to better identify financial crime threats.
- **Complete missing links and make better decisions.** Financial institutions can build networks to form a complete, holistic view of its customers, their relationships, and their activity to make more informed decisions.

BUSINESS CASES

- Anti Money Laundering (AML)
- Internal Fraud - Entitlements
- Credit Card & Transaction Fraud
- Identity Theft & Falsification
- Cyber -Malware
- IoT & Asset Fraud
- Audit & Compliance
- Claim, Dispute Charges
- Law Enforcement-Prosecution

INVESTIGATION - VISUALIZATION

- Advance Visualization
- Dependency | Networking Pathing | Routing | complex Visualization
- Clustering & Community Detection
- Geospatial 'Network Mapping'
- Real Time Data - IoT Systems
- Team-based Workbench & Investigation

ML & ANALYTICS

- Pattern - Recommendations
- What If - Planning & Visibility
- Predictive & Analytics
- Scoring and Risk
- Audit & Compliance - Historical
- Targeting Similarities
- Decision Tree Analytics

Figure 1: Examples of financial uses cases that can be addressed better than before using a combination of graph and artificial intelligence.

Algorithms Empower Investigations

One of the ways to detect fraud is to find groups of transactions or persons that have an unusually high number of interconnections. To detect such groups or communities, you need an algorithm which can efficiently study and assess the entire graph's structure. One such community detection algorithm is Louvain modularity or, simply, the Louvain method.

Louvain has so far been the most effective version of a host of algorithms which try to maximize a score called modularity. Other algorithms, or algorithms which try to shortcut Louvain by using random sampling, either don't get as good scores, don't get consistent scores, or take longer to run.

Other algorithms for working on fraud include PageRank. As an algorithm for determining the influence of web pages based on page-to-page referral, it can also identify who is "pulling the strings" in a community of suspicious financial transactions.

One of the points that is sometimes raised about graph is that people say we can already do fraud detection with SQL queries, which is true when you are looking at a limited number of lookups. This is fine for doing backward analysis where you have an idea of where you want to look for suspicious activity.

However, if you want to examine all connections—as in the case where you don't know which transactions are suspect and you want to find out—that is another case altogether. The SQL query quickly becomes large and unmanageable as the dataset grows because now you want to jump through all of those hops and find out where they went. The problem becomes even more complex because as you work your way through the data, you may need to look left (upstream) and right (downstream) while performing a what-if query—all of which would be complex and difficult to maintain with SQL.

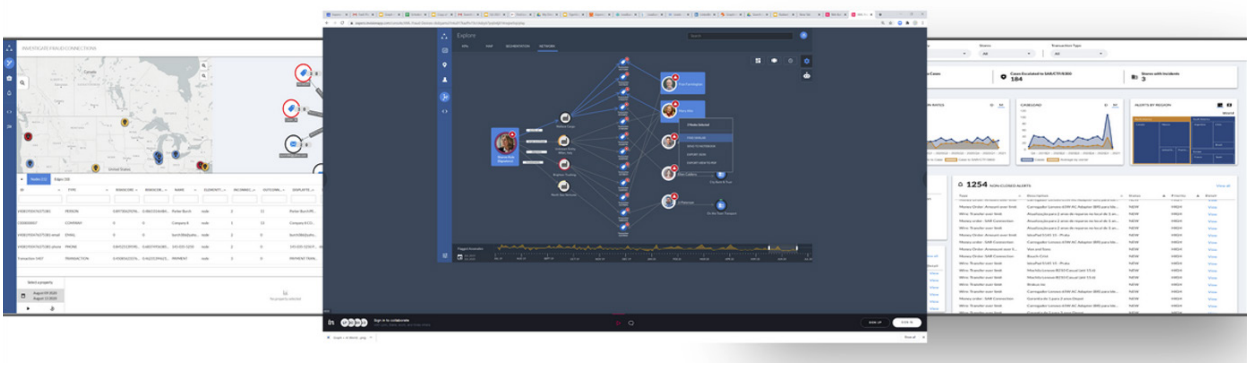

Figure 2: Graph + AI provides for actionable investigative insights informed by deeper and broader analytics

So, three things that push SQL over its limit are the history, the present and the what-if question —together they kill SQL which is why people are looking at graph to solve these problems. As SQL works its way through a tree or network diagram, examining the nodes, fraud queries and algorithms will want to examine nodes to the left and the right of the active node, and a separate SQL query has to be written for each of these hops. To do this, you have to know in advance – which you won't—the structure of the network and which branches and nodes will need to be explored to be able to write the SQL. In some cases, you will need to backtrack and traverse other branches as part of your query which may in turn throw up new paths to traverse

Banks Fight Crime with TigerGraph

One of TigerGraph's banking customers was able to roll out a graph and machine learning solution that enables its compliance team to conduct deeper and broader analyses as part of its anti-money laundering efforts. With the commitment to enhance its AML, the bank saw a significant opportunity in tapping on machine learning to augment and to enhance its existing systems to spot and prevent illicit money flows. The top banking partner made a strategic decision by working with TigerGraph to develop a fit-for purpose AI-driven AML technologies, tools, and systems in a single integrated platform.

TigerGraph differentiates itself from other graph solutions with its ability to scale for massive transaction volume (billions per day) and allowing the largest financial institutions to perform the deepest analytics on a real-time basis. Banks need to take active steps to identify complex activity patterns and anticipate "rare events" to ensure that there are well-designed safeguards and controls and move towards proactive measures to detect and prevent any suspicious activity or respond to evolving regulatory requests. To do so, this will also require a single view of an entire business' portfolio, transactions and operations.

About TigerGraph

TigerGraph is the only scalable graph database for the enterprise. TigerGraph's proven technology connects data silos for deeper, wider and operational analytics at scale. Four out of the top five global banks use TigerGraph for real-time fraud detection. Over 50 million patients receive care path recommendations to assist them on their wellness journey. 300 million consumers receive personalized offers with recommendation engines powered by TigerGraph. The energy infrastructure for 1 billion people is optimized by TigerGraph for reducing power outages. TigerGraph's proven technology supports applications such as fraud detection, customer 360, MDM, IoT, AI, and machine learning. **For more information visit www.tigergraph.com and follow us at:**
Facebook Twitter LinkedIn
Contact us at sales@tigergraph.com

TigerGraph | 3 Twin Dolphin Drive, Suite 225
Redwood City, California 94065
SB-DDAID-111921