ASR Analytics Capability Statement

Graph Analytic Solutions for Fraud Detection

November 2021

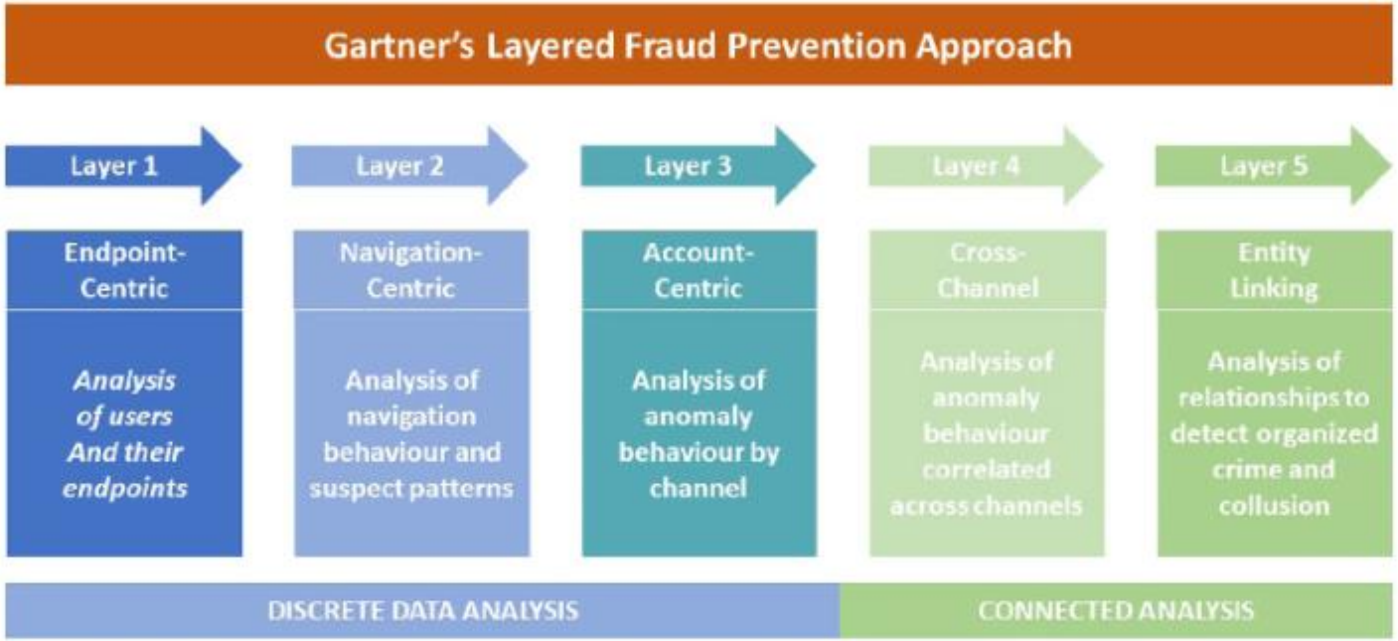
Government agencies can stop undetected fraud and identify unknown risks by building graph databases and conducting network analysis

Problem Statement

- The volume of data needed to manage Government programs is increasing exponentially, particularly in cases where program operations require the analysis of patterns across networks (e.g., related entities, temporal sequence, common geography).
- When organizations are unable to detect these patterns, it can lead to significant blind spots and operational risks (e.g., undetected fraud networks).

Opportunity

- Rapid acceleration in graph analysis capabilities offer an unprecedented opportunity to derive insight about constituent behavior and develop corresponding strategies to promote or enforce compliance with government programs.
- To capitalize on this opportunity, government agencies must have the ability to rapidly create purpose-fit graph databases and conduct network analysis to identify patterns of interest.



Gartner's Layered Fraud Prevention Approach

Layer 1
Endpoint-Centric
Analysis of users And their endpoints

Layer 2
Navigation-Centric
Analysis of navigation behaviour and suspect patterns

Layer 3
Account-Centric
Analysis of anomaly behaviour by channel

Layer 4
Cross-Channel
Analysis of anomaly behaviour correlated across channels

Layer 5
Entity Linking
Analysis of relationships to detect organized crime and collusion

DISCRETE DATA ANALYSIS

CONNECTED ANALYSIS

> *No single layer of fraud prevention or authentication is enough to keep determined fraudsters out of enterprise systems. Organizations should employ a five-layered fraud prevention approach, ranging from basic security measures to complex network analytics.*
>
> **The Five Layers of Fraud Prevention Gartner, Inc. (21 April 2021)**

ASR has developed a suite of open-source tools and analytic services to help government agencies create and analyze networked data

Graph Explorer

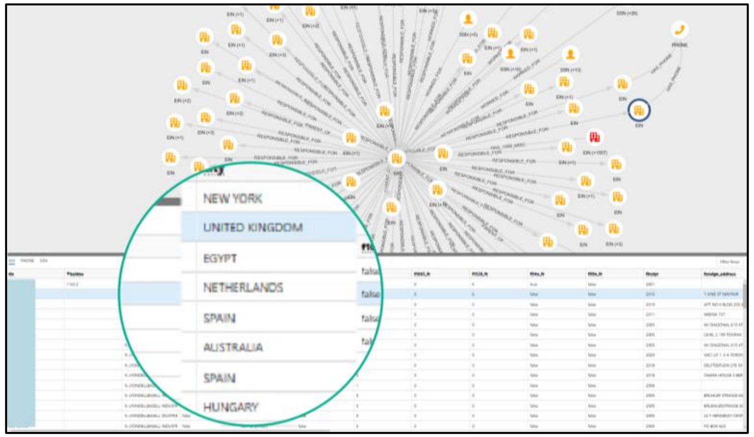
- Graphical user interface that allows users to explore the nodes and edges within the graph, view their attributes, and iteratively expand the graph to explore surrounding entities.
- The IRS has nearly 10,000 distinct users of its Graph Explorer application (mostly investigative analysts working in enforcement functions).
- New graphs are being developed regularly (most recently, a “global high wealth” graph.

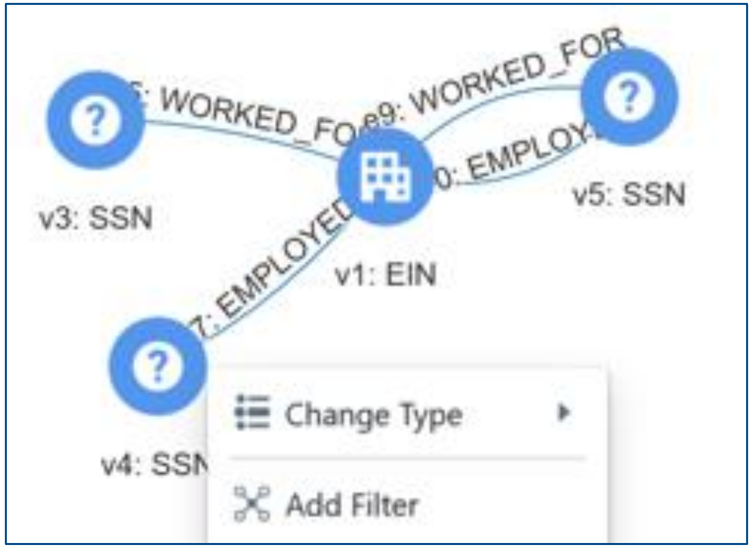
Pattern Matching Tool

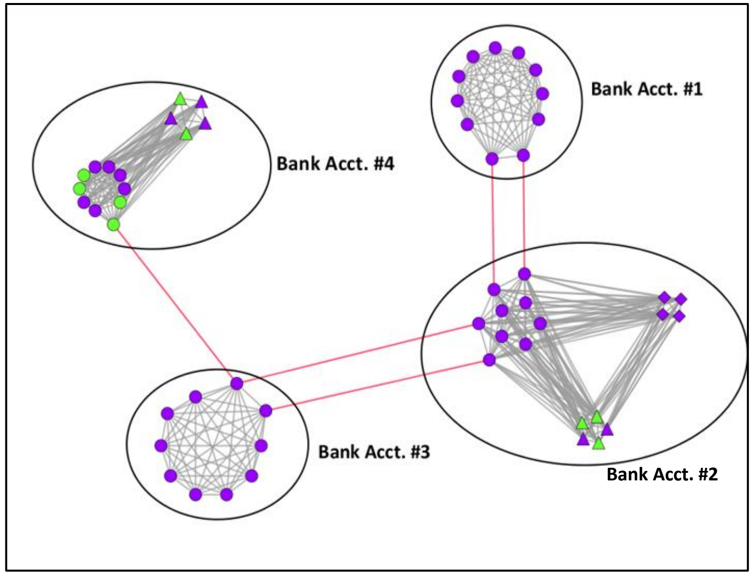
- Graphical user interface that allows users to draw a pattern of interest, search the graph for all instances of that pattern, and filter/rank the resulting cases.
- Enables analysts to quickly assess the scope and scale of known patterns of noncompliance (e.g., non-reciprocal reporting of employment relationships).

Fraud Detection Algorithms

- Machine learning (ML) and artificial intelligence (AI) algorithms (e.g., neural networks, Beta skeleton graphs, conditional random fields) that identify networks of fraud or noncompliance not evident to human analysts.
- These advanced methods have enabled the IRS to identify networks of fraudulent returns missed by traditional methods and reduce the number of false positive selections.



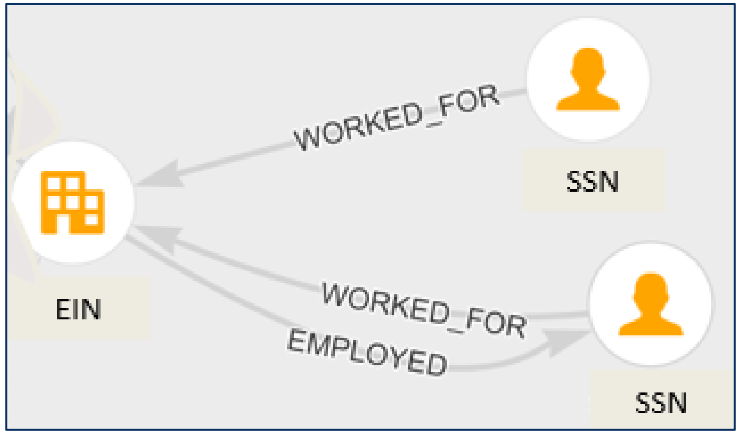




The Pattern Matching Tool can be used with any graph database, which enables rapid deployment across a wide range of domains and data types

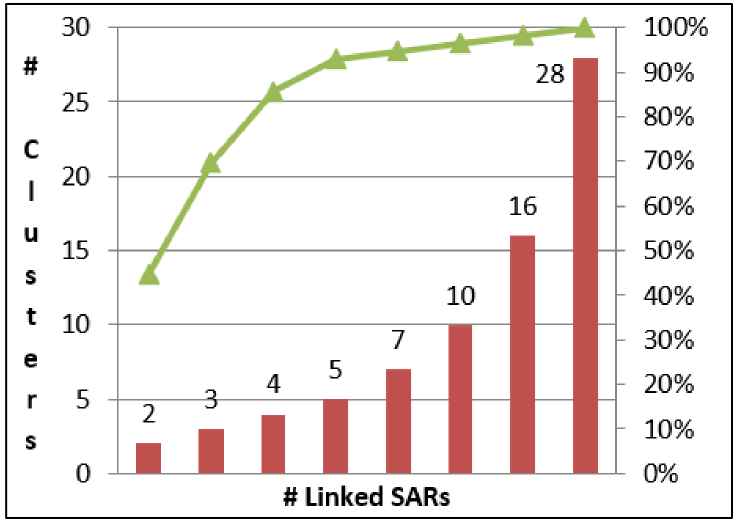
IRS Use Case

- ASR helped the IRS to identify “non-reciprocal employment relationships” (instances where an individual states that they work for a given business, but the business does not report the individual as an employee.
- IRS used the Pattern Match tool to find millions of instances of “non-reciprocal employment relationships”. Nearly 80 thousand employers failed to report any wages paid, despite having employees who reported more than $12 billion in wage income.



FinCEN Use Case

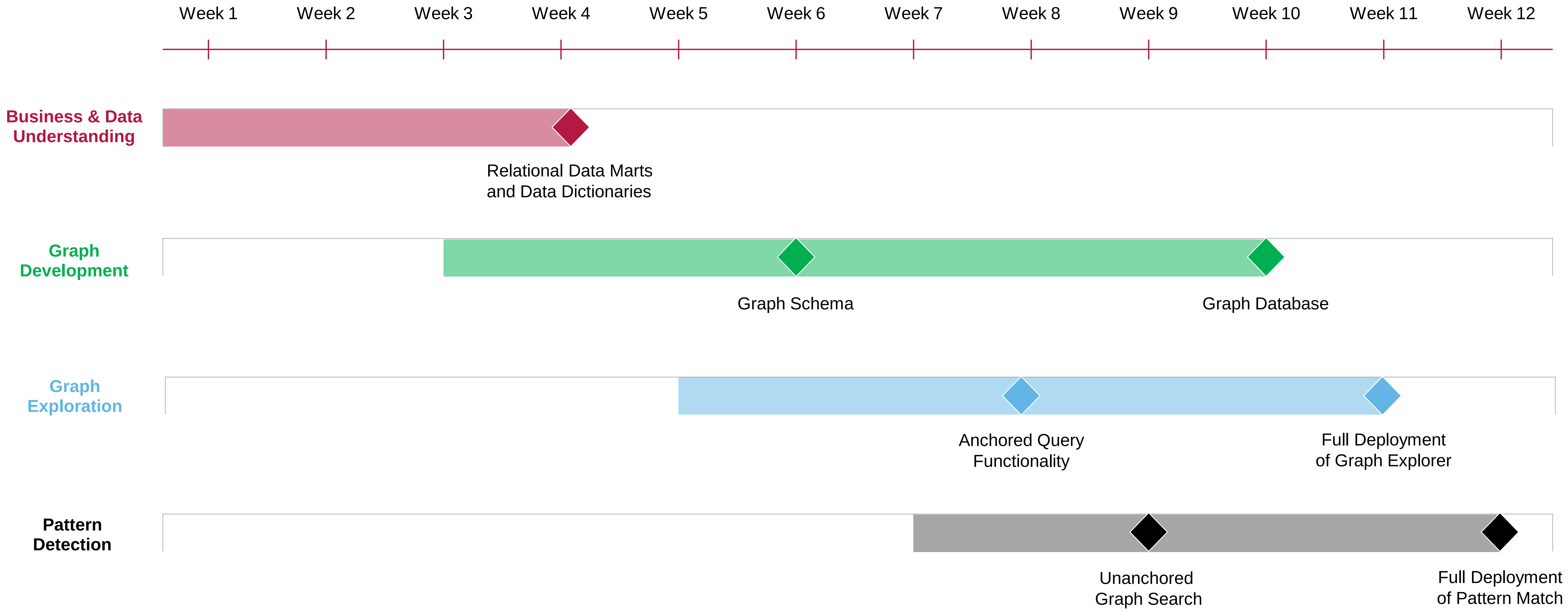
- ASR used data from the IRS and FinCEN to systemically link related Suspicious Activity Reports (SAR).
- ASR used unstructured data from SAR narratives to supplement the structured data and create new links connecting related entities.
- By using methods such as natural language processing (NLP) and social network analysis, ASR was able to identify 30% more suspicious networks than could be identified using structured, tabular data.



Potential Use Cases

- Identify **money laundering** schemes by tracing transactions from entity to entity
- Detect **fraud** when anomalous or suspicious transaction patterns occur
- Build knowledge maps of **institutional data** to provide non-linear, networked documentation
- Guide **criminal investigations** by visualizing the suspect’s entire known network
- Enable **contact tracing** by visualizing relationships within communities
- Map information lineage for **data regulation and privacy protection**
- Analyze network patterns for **cybersecurity and threat detection**
- Compare PII reported in records and filings for **entity resolution**
- Manage **supply chain logistics** by mapping procurement dependencies
- Optimize **business processes** by identifying common dependencies and extraneous events

In most cases, ASR can deploy the Graph Explorer and Pattern Matching applications, and develop an agency-specific prototype, within 12 weeks



Week 1 Week 2 Week 3 Week 4 Week 5 Week 6 Week 7 Week 8 Week 9 Week 10 Week 11 Week 12

Business & Data Understanding

Relational Data Marts and Data Dictionaries

Graph Development

Graph Schema

Graph Database

Graph Exploration

Anchored Query Functionality

Full Deployment of Graph Explorer

Pattern Detection

Unanchored Graph Search

Full Deployment of Pattern Match

ASR Analytics Capability Overview and Contracting Options

Corporate Overview

ASR has been a leading analytic consultancy for nearly 20 years – helping our clients to strengthen fraud prevention and detection, improve organizational planning and performance, and build advanced analytics solutions. We integrate organizational knowledge with evidence-based research and analysis; and we help clients improve operational decision using behavioral insights, predictive analytics, intelligent automation, machine learning, artificial intelligence, natural language processing, pattern analysis, and data visualization.

Government-Wide Contract Vehicles

- **GSA OASIS-SB: Pool 1** #47QRAD20D1197
- **GSA OASIS-SB: Pool 3** #47QRAD20D3164
- **GSA PSS:** #GS10F0062R
- **GSA IT-70:** #GS35F450AA

Corporate Point of Contact

Michael Stavrianos

- 301-758-0371
- *OASIS-SB @asranalytics.com*
- 9466 Georgia Ave. #2025
  Silver Spring MD 20910

Key Capability Areas

Data Engineering

Graph Analytics

Data Visualization

Investigation

Machine Learning

Fraud & Risk Analytics

- **Fraud Detection** – build, maintain, and continuously improve models to detect identity theft and other types of fraud, while conducting research to anticipate emerging threats.
- **Collection Optimization** – design, test, and implement machine- and human-based processes to promote voluntary compliance, optimize enforcement decisions, and increase program efficacy.
- **Case Selection** – build and enhance models to identify the “next best case” across domains (e.g., investigation, enforcement).
- **Customer Persona and Journey Mapping** – improve the customer experience by analyzing historical patterns and nudging customer interaction towards preferred channels.
- **Data Visualization** – create intuitive dashboards that enable mission users to explore operational metrics, trends, and anomalies.
- **Data Engineering & Governance** – build data pipelines to cleanse and integrate enterprise data assets for modeling and analytic programs.
- **Graph Analytics** – build graph databases and pattern detection algorithms for investigative research and network analysis.
- **Analytic Application Development** – develop full-stack solutions using open source and COTS tools to rapidly deploy analytics.

DUNS: *151083305* | **CAGE:** *3XRN0* | **NAICS:** *541611, 541614, 541618, 541990*

Selected Federal Government Clients

U.S. Department of the Treasury

Internal Revenue Service

U.S. Department of Homeland Security

U.S. Department of Commerce

U.S. Department of Defense

U.S. Department of Veterans Affairs