Accertify

Catching E-Commerce Fraud

With Graph Networks

Fraud targeting online merchants is always evolving in terms of the tools and tactics used by attackers. This means defenses also have to grow and change. Graph networks are part of this progression.

Using advanced machine learning (ML), this methodology connects observed behaviors to allow merchants to shut down advanced payment fraud that could slip past other types of defenses.

How do graph networks function, and why are they so useful? Here's the inside story:

1

Don't Judge a Book by Its Cover

The key concept behind graph networks is unsupervised ML, which means finding connections between clusters of similar real-time data, rather than looking at past results.

2

What Are Graphs?

A graph is a model of the relationships between entities.

In retail:
Entity = A transaction.
Relationship = A shared card number, email, or other attribute.

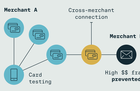
3

Graphs Work By Evolving in Real-Time

New transactions are immediately linked to similar transactions, flagging danger signs in real-time.

They dissolve over time to prevent saturation in risk signals.

4



Graphs Benefit from Consortium Effects

Graphs in use across different merchants can detect suspicious connections between transactions targeting different business.

5

Deep Linking Allows the Discovery of Subtle Patterns

Graph networks can flag risky transactions that are several degrees removed from each other (sharing no common traits) by tracking suspicious relationships.

6

Topologies Reveal Communities Within Transactions

Common shapes created by graphs include:

- **Complete Graphs:** Repeat-customer individuals.
- **Stars:** Households.
- **Connected Stars:** Potential fraudsters with multiple personas.

7

Graph Composites Distinguish Between Fraud and Non-Fraud Patterns

Graph shapes aren't the only warning signs. Potential fraudsters' graphs may contain numerous:

- Email addresses.
- Payment cards.
- Unique devices.
- International physical addresses.

8

Active Research Deepens the Picture

Other factors that can affect the profile of a community include:

- Aggregated past interactions.
- Positive or negative history.

9

Types of Fraud Detected By Graph Networks

Graph networks excel at catching fraudsters engaging in:

- **Real-time stolen card testing.**
- **Synthetic identity use.**
- **Rotating and tumbling of information.**
- **Attempts to cover tracks.**

10

Graphs Can't Catch Every Type of Fraud

When a person only interacts with a merchant once, no graph is created.

Supervised ML methods can defend against threats with no connections.

11

The Difference Between Methods

Graphs model **relationships and behaviors**, while other methods track features and historical patterns.

12

The Future of Graph Network Development

Future applications of graph networks include applying the technology in more places, such as:

- **Behavioral modeling.**
- **Promotional abuse prevention.**
- **Account takeover protection.**

Advanced fraud detection and prevention methods are always evolving, giving companies new items in their toolkits. The deployment of graph networks alongside supervised ML methods allows merchants to stop more types of criminal behavior more effectively, keeping their defenses moving at the speed of right.

Request a demo at accertify.com

Accertify