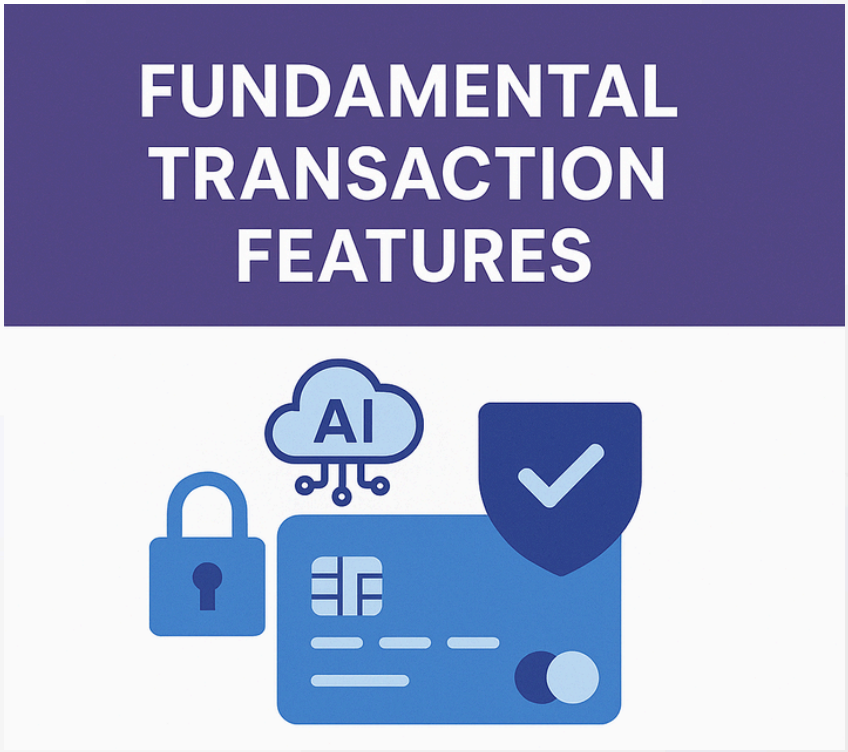
Feature Engineering for Fraud: Crafting the Signals that AI Can Understand - Part 1

- In the ever-evolving landscape of credit and debit card fraud, Artificial Intelligence (AI) stands as a crucial line of defense. However, the ability of AI to effectively detect fraudulent activity hinges on the quality of the data it analyzes.
- At the core of this analysis lie **fundamental transaction attributes**, the basic building blocks that provide the initial context for discerning legitimate transactions from malicious ones.
- While seemingly simple, these **features** are the bedrock upon which more sophisticated fraud detection strategies are built.



The Core Transaction DNA: Initial Clues

Every credit or debit card transaction generates a set of primary data points. These fundamental attributes, though often straightforward, offer vital initial insights for AI models:

- **Transaction Amount:** The Monetary Value.
- This seemingly simple piece of information can be surprisingly telling. Fraudulent transactions often involve amounts that deviate significantly from a cardholder's typical spending habits. An unusually large purchase, especially at an unfamiliar merchant, can be a red flag.
- Conversely, a series of very small, rapid transactions might also indicate a compromised card being tested. AI models are trained to recognize these deviations from established spending patterns, flagging transactions that fall outside the norm.

The Core Transaction DNA: Initial Clues

- **Transaction Time:** The When of the Exchange. The precise timestamp of a transaction provides critical temporal context. Analyzing transaction times allows for several key fraud detection techniques. Sequence analysis examines the order of transactions, looking for suspicious patterns like multiple high-value purchases occurring in rapid succession.
- Velocity checks monitor the number of transactions within a specific timeframe, identifying unusually high activity that might indicate a compromised account. Furthermore, transactions occurring at odd hours, outside a user's typical activity window, can also raise suspicion. AI algorithms learn these temporal patterns, identifying deviations from a user's usual transaction rhythm.

The Core Transaction DNA: Initial Clues

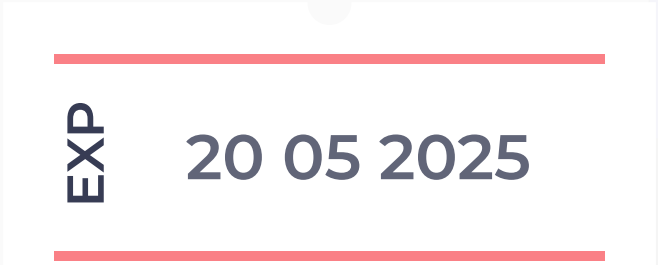
- **Location Data**: Pinpointing the Where. The geographical location of a transaction is a powerful indicator. For card-present (CP) transactions, this is the physical location of the point-of-sale (POS) terminal or ATM. Deviations from the cardholder's usual geographic spending area can be a strong signal of potential fraud. For card-not-present (CNP) transactions, the location is often derived from the Internet Protocol (IP) address of the device used for the purchase. Geographic inconsistencies, such as a transaction originating from a country where the cardholder has no recent travel history, are significant red flags for AI models.

The Core Transaction DNA: Initial Clues

- **Merchant Category Code (MCC)**: Categorizing the Business. This four-digit code classifies the type of business where the transaction occurred. Certain MCCs are historically associated with a higher risk of fraud. For example, merchants dealing in easily resold goods like electronics or jewelry might attract more fraudulent activity. By incorporating MCC into the analysis, AI models can assign a baseline risk score based on the merchant type, adding another layer of context to the transaction.

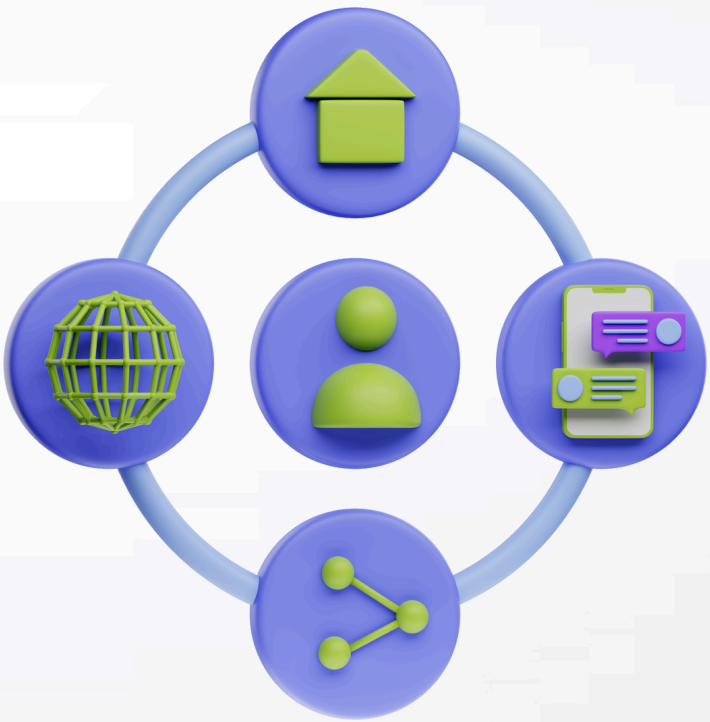
The Core Transaction DNA: Initial Clues

- **Card Information**: The Payment Instrument. Basic details about the payment card itself provide essential context. This includes the card type (credit or debit), which can have different fraud risk profiles.
- The expiration date is crucial for verifying the card's validity. While the full card number is sensitive and often masked, anonymized portions can help in identifying patterns related to specific card ranges or issuers.
- This information helps AI models anchor the transaction to a specific account and identify anomalies related to the card itself.



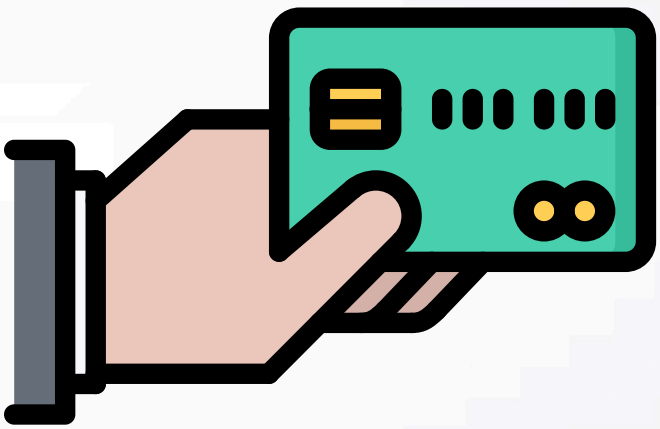
The Core Transaction DNA: Initial Clues

- **Card Information**: While these fundamental attributes provide a crucial starting point, their true power is unlocked when combined with channel-specific indicators and through the application of advanced feature engineering techniques.
- These foundational signals lay the groundwork, providing the initial context that allows AI models to begin distinguishing the subtle differences between a routine purchase and a fraudulent attempt.



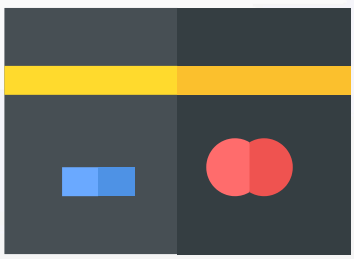
Channeling the Insights: Adding Contextual Depth

- The manner in which a transaction is conducted – whether the **physical card is present or not** – generates unique data points that offer invaluable context for targeted fraud detection.
- Data scientists play a vital role in identifying and incorporating these channel-specific indicators, enriching the information available to AI models.



Channeling the Insights: Adding Contextual Depth

- **Card-Present (CP) Variables**: The Physical Interaction. When a card is physically swiped, inserted, or tapped at a point-of-sale terminal, additional data points become available.
- Features such as the distance from the cardholder's registered home address or the distance from the location of the last legitimate transaction can highlight geographically improbable activity.
- Furthermore, information about the verification methods employed, such as whether the EMV chip was used or if a PIN was required, provides insights into the security protocols of the transaction.
- Even subjective observations about customer behavior at the POS, while less structured, can sometimes offer crucial hints to trained personnel, which can potentially be translated into quantifiable features or used in conjunction with AI alerts.

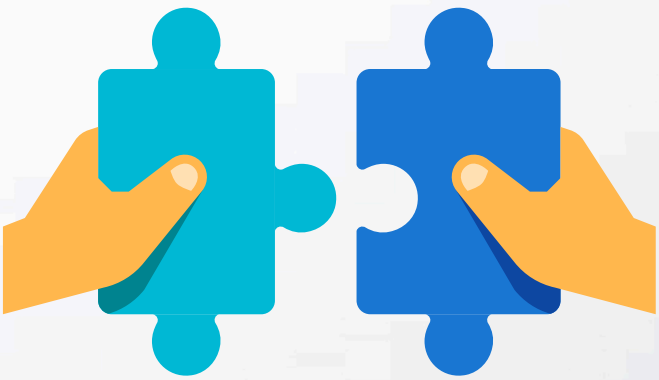


Channeling the Insights: Adding Contextual Depth

- **Card-Not-Present (CNP - E-commerce/Mobile) Variables:** The Digital Footprint. In the realm of online and mobile transactions, the digital footprint becomes paramount.
- Features like the IP address geolocation and device fingerprinting (unique identifiers of the user's device) can help identify suspicious origins or the use of new or unrecognized devices.

Channeling the Insights: Adding Contextual Depth

- **Card-Not-Present (CNP - E-commerce/Mobile) Variables:**
- Discrepancies between the billing and shipping addresses, multiple orders shipping to the same address with different cards, or a single card shipping to numerous addresses can all be strong indicators of fraud. The verification of the CVV code and the validity and reputation of the email address used in the transaction add further layers of scrutiny.
- Moreover, order characteristics, such as unusually large quantities of high-value items or requests for expedited shipping, can also contribute to a richer picture of the transaction's risk. Finally, the outcome of 3D Secure authentication (e.g., successful verification or failure) provides a direct signal of an additional security layer's effectiveness.



Channeling the Insights: Adding Contextual Depth

- **Card-Not-Present (CNP - MOTO) Variables**: Remote Interactions. For mail order and telephone order transactions, where the card is not physically present and interaction is remote, the available data for real-time verification is often limited.
- In these scenarios, features like the Address Verification Service (AVS) match result and whether the CVV code was provided become critical signals.
- The details provided by the customer over the phone or mail, such as the name on the card, account number, and expiration date, are also crucial and can be checked for inconsistencies or anomalies.

Summary

- By meticulously identifying and incorporating these channel-specific variables, data scientists provide AI models with the nuanced context necessary to differentiate legitimate customer behavior from the diverse tactics employed by fraudsters across different transaction environments.
- This layered approach, starting with fundamental attributes and enriched with channel-specific insights, forms a robust foundation for effective fraud detection.

Special Thanks to ChatGPT and Gemini for Content support