Rules

1. What are the different inputs that can be passed into rules?

A. Lists, AI scores, event information, velocities, external calls.

B. In Microsoft Dynamics 365 Fraud Protection, you can create rules that utilize various inputs to convert an assessment into a decision, such as Approve, Reject, Review, or Challenge. The inputs for these rules can include:

   a. Attributes sent in the API request for the assessment, including custom data which can be accessed with the @ operator. For example, @"user.userId".
   b. Scores generated from Fraud Protection's artificial intelligence models, such as @"riskscore".
   c. Lists that you have uploaded to Fraud Protection. You can reference these lists in your rules after uploading them.
   d. Velocities that you have defined in Fraud Protection to perform velocity checks.
   e. External calls that you have created in Fraud Protection.
   f. Functions that you have created within Fraud Protection.

C. Rules are defined using the RETURN and WHEN keywords, where the RETURN statement specifies the decision and is only executed if the WHEN statement evaluates to True. The WHEN statement specifies a Boolean condition that determines if the RETURN statement executes. Expressions can be compared using comparison operators (such as ==, !=, >, <), and can be combined using logical operators such as and (&&) and or (||).

D. For more detailed information, you can refer to the official documentation on Manage rules - Dynamics 365 Fraud Protection | Microsoft Learn which provides a comprehensive guide on how to manage rules within the system.

E. References:

   a. [1] Manage rules - Dynamics 365 Fraud Protection | Microsoft Learn

2. What kind of rules are commonly used to fight fraud?

A. In Microsoft Dynamics 365 Fraud Protection, you can create rules that utilize various inputs to convert an assessment into a decision, such as Approve, Reject, Review, or Challenge. The inputs for these rules can include:

   a. Attributes sent in the API request for the assessment, including custom data which can be accessed with the @ operator. For example, @"user.userId".
   b. Scores generated from Fraud Protection's artificial intelligence models, such as @"riskscore".
   c. Lists that you have uploaded to Fraud Protection. You can reference these lists in your rules after uploading them.
   d. Velocities that you have defined in Fraud Protection to perform velocity checks.
   e. External calls that you have created in Fraud Protection.
   f. Functions that you have created within Fraud Protection.

B. Rules are defined using the RETURN and WHEN keywords, where the RETURN statement specifies the decision and is only executed if the WHEN statement evaluates to True. The WHEN statement specifies a Boolean condition that determines if the RETURN statement executes. Expressions can be compared using comparison operators (such as ==, !=, >, <), and can be combined using logical operators such as and (&&) and or (||).

C. For more detailed information, you can refer to the official documentation on Manage rules - Dynamics 365 Fraud Protection | Microsoft Learn which provides a comprehensive guide on how to manage rules within the system.

3. What is the impact on latency for all my current rules?

A. The impact on latency for rules in Microsoft Dynamics 365 Fraud Protection can vary based on the complexity and number of rules you have in place. Generally, the system is designed for elastic scale using Microsoft Azure, and larger customers regularly sustain rates of over **60 transactions per second (TPS) for purchases** and **200 TPS overall** with P95 latencies of **625ms and 550ms**, respectively.
B. For a more detailed analysis of your current rules' performance, including latency, you can utilize the **Rule analyst reports** provided by Fraud Protection. These reports are designed to track the impact of the rules you've enabled, helping you understand the transaction volume, distribution, and potential fraud trends by rule and clause. They also allow you to analyze decisions and performance by rule segment and compare the impact of observe rules and decision rules.
C. If you're looking for real-time updates or specific latency metrics for your current rules, it's recommended checking the latest statistics on the Dynamics 365 Fraud Protection dashboard or consulting with your team members who might have access to up-to-date performance data.

References

D. Rule analyst reports - Dynamics 365 Fraud Protection | Microsoft Learn

4. Why did this transaction not hit rule X?

There could be several reasons why a transaction did not trigger a specific rule (Rule X) in Microsoft Dynamics 365 Fraud Protection. Here are some common factors to consider:

- Rule Configuration: Ensure that Rule X is correctly configured with the appropriate conditions and logic. If the conditions are not met, the rule will not trigger.
- Rule Order: The order of rules matters. If Rule X is lower in the order and a previous rule has already made a decision on the transaction, Rule X may not be evaluated.
- Rule Scope: Check if Rule X is scoped correctly to apply to the transaction in question. It might be limited to certain types of transactions or channels.
- Data Availability: The necessary data to evaluate Rule X must be present in the transaction. If the required data is missing or incorrect, the rule may not trigger.
- Rule Status: Verify that Rule X is active and not disabled or in 'observe' mode, which would prevent it from taking action on transactions.

For a specific transaction, you can review the Rule analyst reports and Summary report in Dynamics 365 Fraud Protection, which provide insights into the transaction volume, rule decision distributions, and the impact of rules that you've enabled [1][2]. These reports can help you understand why Rule X did not trigger for a particular transaction.

If you're still unable to determine why Rule X did not hit, you may need to consult with your Dynamics 365 Fraud Protection support team or review the service logs for more detailed information. There might have been a recent update or an issue escalated that could be related to the rule's behavior.

Remember to consider any recent changes in the Fraud Protection system or updates in the rules that might affect the transaction flow.

References:
[1] Rule analyst reports - Dynamics 365 Fraud Protection | Microsoft Learn
[2] Summary report - Dynamics 365 Fraud Protection | Microsoft Learn

5. Can you find out the common rules for the transactions that had the highest scores?

   In Microsoft Dynamics 365 Fraud Protection, transactions with the highest scores are typically those that are most likely to be fraudulent. The common rules applied to these transactions are designed to identify and prevent high-risk activities. Here are some of the rules that are commonly used:

   - Threshold rules: These rules reject transactions that exceed a certain risk score. For example, transactions for gift cards might be rejected if the risk score is above 400.
   - Velocity rules: These rules identify and block rapid, repeated transactions from the same entity, which could indicate fraudulent behavior.
   - List checks: These rules compare transaction data against lists of known fraud indicators, such as device fingerprints or IP addresses.
   - Anomaly detection: These rules look for patterns of behavior that are unusual and deviate from the norm, which could indicate fraud.

   For a more detailed understanding of the common rules applied to high-scoring transactions, you may want to review the "Score analyst reports" in the Dynamics

365 Fraud Protection portal, which can provide insights into the relationship between Fraud Protection scores and the rules that were executed.

References:

- Score analyst reports - Dynamics 365 Fraud Protection | Microsoft Learn

6. What rule can help catch more fraud based on past data?

In Microsoft Dynamics 365 Fraud Protection, transactions with the highest scores are typically those that are most likely to be fraudulent. The common rules applied to these transactions are designed to identify and prevent high-risk activities. Here are some of the rules that are commonly used:

- Threshold rules: These rules reject transactions that exceed a certain risk score. For example, transactions for gift cards might be rejected if the risk score is above 400.
- Velocity rules: These rules identify and block rapid, repeated transactions from the same entity, which could indicate fraudulent behavior.
- List checks: These rules compare transaction data against lists of known fraud indicators, such as device fingerprints or IP addresses.
- Anomaly detection: These rules look for patterns of behavior that are unusual and deviate from the norm, which could indicate fraud.

For a more detailed understanding of the common rules applied to high-scoring transactions, you may want to review the "Score analyst reports" in the Dynamics 365 Fraud Protection portal, which can provide insights into the relationship between Fraud Protection scores and the rules that were executed

References:

- Score analyst reports - Dynamics 365 Fraud Protection | Microsoft Learn

7. How inheritance works for rules?

In Microsoft Dynamics 365 Fraud Protection, rule inheritance works within a multi-environment hierarchy. If your Fraud Protection instance has multiple environments, you can manage rules in a specific environment using the environment switcher. Rules in the top-level parent environment are evaluated first. If the rule settings for the top-level parent environment are set to "Run all matching rules until a decision is made," the rules in the second-level parent environment are evaluated next. This process continues unless the rule settings for an environment are set to "Run only the first matching rule," or until all the rules for the parent environment and the current environment are evaluated [1].

However, it's important to note that all resources, such as velocities, external calls, lists, and external assessments, are always local to an environment. Even in a hierarchy, resources defined in a parent environment are not inherited for use in rules in child environments. They are inherited for aggregation purposes but not for use in rules. For example, a velocity defined in a parent environment would increment based on transactions to a child environment, but if you wanted to reference that velocity in a rule, the rule would have to be in the same (parent) environment [2].

For functions, you can create them in any environment in the multi-hierarchy stack. When a function references resources available in the environment, the lower environments that invoke the function also inherit the resources that the function references

For a more detailed understanding of how inheritance works for rules in Microsoft Dynamics 365 Fraud Protection, you can refer to the official documentation on Manage rules - Dynamics 365 Fraud Protection | Microsoft Learn

References

- [1] Manage rules - Dynamics 365 Fraud Protection | Microsoft Learn
- [2] Functions - Dynamics 365 Fraud Protection | Microsoft Learn

8. By mistake, I marked a transaction as approved, now I want to change that decision. Can I do it?

In Microsoft Dynamics 365 Fraud Protection, once a transaction has been marked as approved, it may not be possible to change the decision directly within the system due to the nature of transaction processing and the potential impact on customer experience and reporting. However, there are steps you can take to address the situation:

- Review the transaction: Investigate the transaction details to understand why it was mistakenly approved. This can help prevent similar issues in the future.
- Manual intervention: If the transaction has not yet been fully processed or settled, you may be able to manually intervene with your payment processor or bank to stop or reverse the transaction.

- Update your rules: To prevent future occurrences, review and update your fraud protection rules to ensure they are correctly configured to flag similar transactions for review or rejection.
- Customer support: If the transaction has already been completed, you may need to contact the customer to resolve the issue, which could involve refunding the transaction or other customer service actions.

For specific guidance on managing such situations, you can refer to the Dynamics 365 Fraud Protection documentation or reach out to the support team for assistance. Additionally, within your organization, you may have protocols or documentation on how to handle post-approval changes, which could provide further insights [1][2][3].

If you need to update a customer's status or a transaction decision, you may follow the steps outlined in the Dynamics 365 Fraud Protection documentation, which includes editing the default support rule or creating a new rule for users with a status of "Watch".

For a detailed understanding of the capabilities and limitations regarding transaction decisions in Dynamics 365 Fraud Protection, you can consult with your colleagues who specialize in this area.

References:

- [1] Manage custom lists - Dynamics 365 Fraud Protection | Microsoft Learn
- [2] Score analyst reports - Dynamics 365 Fraud Protection | Microsoft Learn
- [3] Manage rules - Dynamics 365 Fraud Protection | Microsoft Learn

9. Can you recommend some rules that can effectively protect our business?

In Microsoft Dynamics 365 Fraud Protection, there are several rules that can be implemented to effectively protect your business from fraudulent activities. Here are some recommendations based on best practices and your company's internal resources:

- Adaptive AI technology: Utilize Adaptive AI technology to combat purchase, account, and omni-channel return and discount fraud. This technology helps balance revenue opportunity vs. fraud loss and checkout friction.
- Purchase Protection: Implement Purchase Protection to improve the acceptance rate of e-commerce transactions with insights and tools that help protect revenue.

- Account Protection: Use Account Protection to prevent fraudulent account creation, account takeover, and ensure sensitive information such as free trials, loyalty points, and consumer data aren't abused.
- Loss Prevention: Leverage Loss Prevention to identify anomalies and potential fraud on returns and discounts arising from omni-channel purchases, enabling quick action to mitigate losses.
- Threshold rules: Create rules that use the score generated by Fraud Protection's AI model, together with additional parameters from the request payload, to make decisions such as Approve, Reject, Review, or Challenge.
- Velocity checks: Define velocities in Fraud Protection to perform velocity checks and identify rapid, repeated transactions from the same entity.
- List checks: Upload lists to Fraud Protection and reference these lists in your rules to compare transaction data against known fraud indicators.
- Device fingerprinting: Help protect accounts with device fingerprinting to identify and block devices associated with fraudulent activities.
- Bot protection: Configure the engine to match your business needs and help defend accounts with bot protection.

For a comprehensive guide on how to manage rules within the system, you can refer to the official documentation on Manage rules - Dynamics 365 Fraud Protection | Microsoft Learn.

Additionally, within your organization, you may find valuable insights and guidance on rule management in the Dynamics Fraud Protection presentation, which discusses comprehensive rule engines that allow you to create from simple rules to complex rules in decisioning mode or observation mode by incorporating ML risk scores, lists, velocities, and other enrichment data from your own external calls.

References:

- Manage rules - Dynamics 365 Fraud Protection | Microsoft Learn

10. How often should we revisit the rule and make adjustment?

In Microsoft Dynamics 365 Fraud Protection, it's important to regularly revisit and adjust rules to ensure they remain effective against evolving fraud patterns. While there is no one-size-fits-all answer, here are some best practices:

- Regular Review: Rules should be reviewed on a regular basis, such as monthly or quarterly, to ensure they align with current fraud trends and business strategies.

- Performance Analysis: Utilize the Rule analyst reports to monitor the performance and impact of your rules. Adjustments may be necessary if you notice changes in fraud patterns or false positive rates.
- After Major Events: Review and potentially adjust rules after major events such as product launches, holiday seasons, or known fraud attacks, as these can change the fraud landscape significantly.
- Feedback Loop: Incorporate feedback from customer service and fraud investigation teams into your rule adjustments to address any new types of fraud they are encountering.

It's also beneficial to stay informed about updates to Dynamics 365 Fraud Protection features and capabilities, as new functionalities may offer additional ways to enhance your rules and fraud protection strategies.

References:

- Manage rules - Dynamics 365 Fraud Protection | Microsoft Learn