External Calls

1. What 3rd party data providers do you connect to as standard? For what purpose?

   Microsoft Dynamics 365 Fraud Protection connects with various third-party data providers as part of its standard operations to enhance fraud protection capabilities. These providers offer additional data points that can be used to assess and score transactions for potential fraud risks. The purpose of integrating with these data providers is to leverage their databases and services to enrich the information available for fraud assessment, thereby improving the accuracy and effectiveness of fraud detection mechanisms.

   While specific third-party providers are not listed in the provided data, the system is designed to work with external organizations to process, transmit, or store data as necessary for fraud protection services. The integration with these providers allows Dynamics 365 Fraud Protection to access a broader range of data, including but not limited to credit and payment history, device reputation, and other relevant information that can contribute to a comprehensive fraud assessment.

   For detailed information on which third-party data providers are connected and for what specific purposes, you may refer to the official Dynamics 365 Fraud Protection documentation.

2. Is there a best practice or workaround for any errors & exceptions that occur for External Calls? Context: instrument a feedback loop for either resolving the error or implement a workaround (i.e. creating another rule to resolve issues where External calls return with HTTP error codes or latency or network issues).

   You can specify a default response in case an external call fails. Based on that, you can write a different rule of any sort. For example, if External call “A” fails, we can write a rule to send back "Review" with reason as "A failed”. But you could also try and use a different provider via External call.

3. If there are issues with External calls, please confirm that any rules defined afterwards still execute? If so, what occurs if the subsequent rule(s) need information or data from the prior failed External calls? Valid scenario?

Yes, they still execute, but the "default" response you specify when creating the external call is used to execute the rest of the rules.

4. What is the External Call feature in Dynamics Fraud Protection?

   The External Call feature in Microsoft Dynamics 365 Fraud Protection allows you to ingest data from APIs outside of Dynamics 365 Fraud Protection and use that data to make informed decisions in real-time. This feature can connect to any API endpoint, make a request to that endpoint as required by your rules, and use the response from that endpoint to make a decision. For example, you might use third-party address and phone verification services, or your own custom scoring models, which could provide critical input that helps determine the risk level for some events [1].

   To create an external call, you would go to the Fraud Protection portal, select External Calls, and then create a new external call. You can set parameters to pass data from Fraud Protection to your API endpoint, and these parameters are sent to the endpoint either in the query string or as part of the request body depending on the HTTP method selected. Fraud Protection currently supports various authentication methods for these calls, including Anonymous, Basic, Certificate, OAuth (Microsoft Entra ID), OAuth (Generic), and OAuth (Custom token), and supports the HTTP methods GET and POST [1].

   References:

   - [1] External calls - Dynamics 365 Fraud Protection | Microsoft Learn

5. How can I use the External Call feature to make more informed decisions?

   The External Call feature in Microsoft Dynamics 365 Fraud Protection allows you to enhance your fraud detection capabilities by integrating data from external APIs into your decision-making processes. Here's how you can use it to make more informed decisions:

   - **Data Enrichment**: Use External Calls to bring in additional data points from third-party services, such as address verification or custom scoring models, which can provide valuable insights into the risk level of transactions [1].
   - **Custom Rules**: Create custom rules that trigger External Calls based on specific conditions within your transactions. This allows you to dynamically fetch data that can influence the outcome of fraud assessments [1].

- **Real-Time Decisions**: Since External Calls can be made in real-time within your rules, you can use the responses to immediately impact the decision process, such as accepting, rejecting, or flagging transactions for review [1].
- **Testing and Monitoring**: After setting up External Calls, test them to ensure they are working as expected. Monitor their performance and the quality of data they provide to continuously refine your fraud protection strategies [1].
- **Feedback Loop**: Use the results from External Calls to feed back into your machine learning models, helping them to learn and adapt to new patterns of fraud based on the enriched data [1].
- **Documentation and Support**: Refer to the official Dynamics 365 Fraud Protection documentation for detailed guidance on creating, testing, and monitoring external calls. Reach out to your internal support team or top collaborators for assistance
- By effectively utilizing the External Call feature, you can significantly improve the precision of your fraud protection measures and adapt more quickly to emerging fraud trends. Remember to review the documentation and collaborate with your team for the best implementation strategies.

  References:
- [1] External calls - Dynamics 365 Fraud Protection | Microsoft Learn

6. Can I customize the data I bring in through External Calls?

   Yes, in Microsoft Dynamics 365 Fraud Protection, you can customize the data you bring in through External Calls. You have the flexibility to define the parameters and the data that you pass to your API endpoint. Depending on the HTTP method you select, these parameters are sent to the endpoint either in the query string or as part of the request body. You can manually add parameters defined in this step to the request URL, header, and/or body using the format {parameter.<parameter name>}. All parameter values are interpreted as strings, and you can add sample values for each parameter that Fraud Protection uses to make a sample call to your endpoint [1].

   This customization allows you to ingest data from APIs outside Microsoft Dynamics 365 Fraud Protection and then use that data to make informed decisions in real-time. For example, you might use third-party address and phone verification services, or your own custom scoring models, which could provide critical input that helps determine the risk level for some events [1].

References:

- [1] External calls - Dynamics 365 Fraud Protection | Microsoft Learn

7. Where can I find more information on how to set up and use External Calls?

   For detailed information on how to set up and use External Calls in Microsoft Dynamics 365 Fraud Protection, you can refer to the following resources: The official Microsoft Learn documentation provides a comprehensive guide on External Calls, including types of APIs that can be used, how to create, test, monitor, and manage external calls, and how to use them in rules. You can find this guide here. These resources should provide you with the necessary information to set up and effectively use External Calls in Dynamics 365 Fraud Protection.

   References:

- External calls - Dynamics 365 Fraud Protection | Microsoft Learn

8. What APIs are used for External Calls?

   In Microsoft Dynamics 365 Fraud Protection, External Calls can be used to ingest data from various APIs outside of Dynamics 365 Fraud Protection to make informed decisions in real-time. The types of APIs that can be used in an external call include third-party address and phone verification services, or your own custom scoring models, which might provide critical input that helps determine the risk level for some events. The system currently supports the following authentication methods for these calls: Anonymous, Basic, Certificate, OAuth (Microsoft Entra ID), OAuth (Generic), and OAuth (Custom token). It also supports the HTTP methods GET and POST. For example, you might have an API endpoint called "Custom Assessment" that you need to call to get device fingerprinting data back. This involves creating a new "custom" in the DFP portal.

   References:

- External calls - Dynamics 365 Fraud Protection | Microsoft Learn

9. How do I create an External Call?

   Creating an external call in Microsoft Dynamics 365 Fraud Protection allows you to ingest data from APIs outside the system and use that data to make informed decisions in real time. Here's a step-by-step guide to help you create an external call:

- Access the Fraud Protection Portal: Navigate to the Fraud Protection portal and select 'External Calls' from the left navigation.
- Create a New External Call: Click on 'New external call' to start setting up your external call.
- Configure the External Call:
  - **Name**: Enter a name for your external call. This name will be used to reference the call from your rules.
  - **Description**: Provide a description to help identify the external call.
  - **Add Parameter**: Use parameters to pass data from Fraud Protection to your API endpoint. Parameters are sent in the query string or request body depending on the HTTP method selected.
  - **Add Configuration**: Provide fixed configuration data on the setup page.
  - **Test the Connection** (Optional): Before creating the external call, you can test the connection to your API endpoint.
- Create the External Call: After setting the required fields, select 'Create' to finalize the external call [1].
- Save and Use the External Call: After successful testing, save the external call. You can then reference this call in your decision rules to use the data returned by the external service in your fraud protection logic.
  Remember, Fraud Protection currently supports authentication methods like Anonymous, Basic, Certificate, OAuth (Microsoft Entra ID), OAuth (Generic), and OAuth (Custom token), and HTTP methods GET and POST.

For a detailed explanation and additional guidance, you can refer to the official Microsoft documentation on managing external calls in Dynamics 365 Fraud Protection. If you need additional assistance please contact your Microsoft authorized partner or Microsoft support.

References:

- External calls - Dynamics 365 Fraud Protection | Microsoft Learn

10. How do I test that the External Call is working?

To test that an External Call is working in Microsoft Dynamics 365 Fraud Protection, you can follow these steps:

- Navigate to the Fraud Protection portal and go to the **External Calls** section.

- Select the external call you want to test or create a new one if necessary.
- Fill in all the required fields for the external call setup.
- Click on **Test connection** to send a sample request to your API endpoint [1].

  This will help ensure that Dynamics 365 Fraud Protection can connect to your endpoint and that the external call is set up correctly. If the test is successful, you will receive a response from the API endpoint. If there are any issues, the portal will provide error messages that can help you troubleshoot the problem.

  References:
- [1] External calls - Dynamics 365 Fraud Protection | Microsoft Learn