

# Modo Mail Bulk

En Postman cree una nueva consulta, configure los headers **username**, **password** y **Content-Type** según la información de su instancia The Fraud Explorer.

Escriba en la URL la dirección <https://suinstancia/rest/fraudTriangleMailBulk>, seleccione el método **POST** y luego en la pestaña **BODY** agregue cada evento de forma numérica así:

```
{
  "1":
  {
    "ownerName": "John Doe",
    "mailDate": "2-28-2023 3:07:38 PM",
    "businessUnit": "BASELINE",
    "llmEngine": "yes",
    "mailFrom": "John Doe",
    "mailTo": "Jason Emerald",
    "mailSubject": "Problemas en puerto",
    "phrases": "Buenos dias, tenemos problemas con el barco en el puerto de llegada, hay que darle un billete a los inspectores para que no nos frenen el desembarco. Recuerden que esto lo deben hacer con cuidado para que nadie se de cuenta"
  },
  "2":
  {
    "ownerName": "John Doe",
    "mailDate": "2-28-2023 11:39:20 AM",
    "businessUnit": "BASELINE",
    "llmEngine": "yes",
    "mailFrom": "John Doe",
    "mailTo": "Mary Stewart",
    "mailSubject": "Devolución de mercancía",
    "phrases": "Hola Mary, vende la mercancía, luego devuélvela y reclama la comisión. Son ventas ficticias pero no hay problema porque acá en la empresa permiten hacer devoluciones. Hazlo para cumplir las metas y que puedas comisionar."
  }
}
```

Luego de clic en el botón **Send** y verá cómo retorna un análisis del contenido semántico:

The screenshot shows a Postman interface for a POST request to `https://demo.thefraudexplorer.com/rest/fraudTriangleMailBulk`. The request body is a JSON array of two mail objects. The response is a JSON object with the following structure:

```
1  {
2  "1":
3  {
4    "ownerName": "John Doe",
5    "mailDate": "2-28-2023 3:07:38 PM",
6    "businessUnit": "BASELINE",
7    "llmEngine": "yes",
8    "mailFrom": "John Doe",
9    "mailTo": "Jason Emerald",
10   "mailSubject": "Problemas en puerto",
11   "phrases": "Buenos dias, tenemos problemas con el barco en el puerto de llegada, hay que darle un billete a los inspectores para que no
12             nos frenen el desembarco. Recuerden que esto lo deben hacer con cuidado para que nadie se de cuenta"
13   },
14   "2":
15   {
16     "ownerName": "John Doe",
17     "mailDate": "2-28-2023 11:39:20 AM",
18     "businessUnit": "BASELINE",
19     "llmEngine": "yes",
20     "mailFrom": "John Doe",
21     "mailTo": "Mary Stewart",
22     "mailSubject": "Devolución de mercancía",
23     "phrases": "Hola Mary, vende la mercancía, luego devuélvela y reclama la comisión. Son ventas ficticias pero no hay problema porque aca
24               en la empresa permiten hacer devoluciones. Hazlo para cumplir las metas y que puedas comisionar."
25   }
26 }
```

The response status is 200 OK, with a time of 14.69 s and a size of 2.55 KB. The response body is shown in JSON format:

```
1  {
2  "id": 1,
3  "mailOwner": "John Doe",
4  "mailDate": "2-28-2023 3:07:38 PM",
```

Este servicio de **Mail** en modo **BULK** entrega información de la cantidad de comportamientos expresados en correos electrónicos basados en el triángulo del fraude (presión, oportunidad y justificación), así como una probabilidad, acompañado de un análisis de tono y de intimidad.

Los insights también entregan información de valor agregado, como el análisis de pronombres personales (honestidad), detección de criticidad (alta o baja), un resumen de los tópicos del evento analizado, una clasificación de comportamientos, un inventario de riesgos y un match de frases en el contenido semántico.

**The Fraud Explorer** es un software que junto con **FraudGPT** detecta el fraude y la corrupción en las organizaciones. Este software está siendo desarrollado por **NOFRAUD.la**. Este contenido es privado y únicamente está disponible para clientes de NOFRAUD. Está prohibida su publicación en fuentes abiertas o disponibles al público.

Revision #2

Created 23 July 2025 03:23:31 by Julian Rios

Updated 26 July 2025 02:39:08 by Julian Rios