NVDIA NIM-FRAUD BLUEPRINT

🛑 Problema

El fraude en transacciones con tarjetas de crédito representa una amenaza creciente para las instituciones financieras. Se proyecta que las pérdidas globales superen los **403 mil millones de dólares en la próxima década**. Los sistemas tradicionales de detección basados en reglas o métodos estadísticos son **reactivos, limitados e insuficientes** frente a los esquemas de fraude modernos, cada vez más sofisticados y difíciles de identificar.

🎯 Objetivo de la solución.

Proporcionar a las instituciones financieras una metodología moderna, inteligente y proactiva para detectar y prevenir actividades fraudulentas. La solución —basada en el NVIDIA AI Blueprint— ofrece un flujo de trabajo completo que utiliza:

- Graph Neural Networks (GNNs) para mejorar la precisión en la detección del fraude.
- NVIDIA Financial Fraud Detection Container para entrenar modelos avanzados.
- NVIDIA Dynamo-Triton (Triton Inference Server) para inferencia de alta velocidad y explicable.
- Generación automática de archivos de configuración necesarios para acelerar la puesta en producción.

✅ Resultados de la solución

- Detectar fraudes complejos con mucha mayor precisión que los modelos tradicionales.
- Reducir drásticamente los falsos positivos, aumentando la eficiencia operativa y la experiencia del cliente.
- Generar fraud scores para priorizar casos críticos.
- Integrar todo el pipeline de manera rápida gracias a los contenedores optimizados de NVIDIA, tanto para entrenamiento como para inferencia.

📈 Impacto esperado

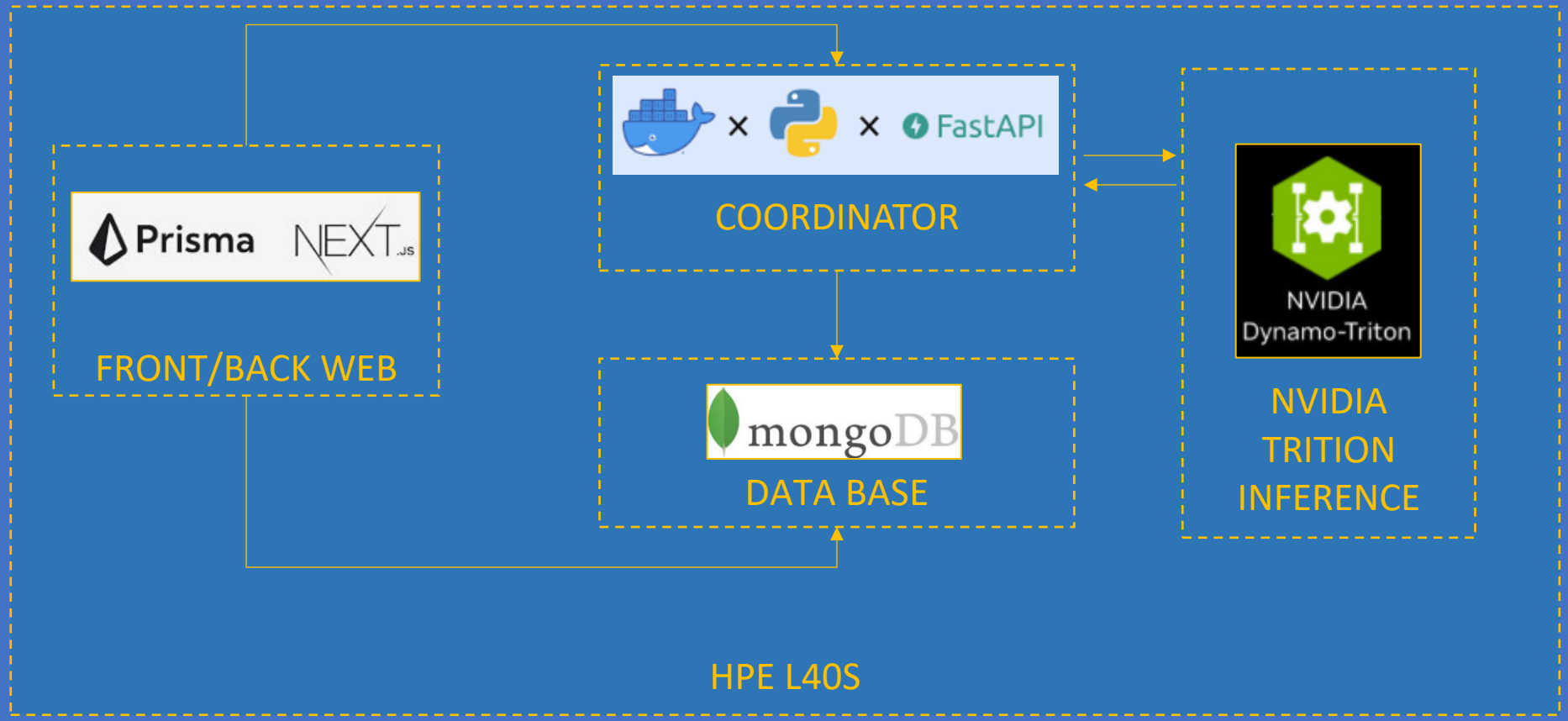
- Disminución significativa de pérdidas financieras, al identificar patrones de fraude antes de que ocurran transacciones dañinas.
- Mayor precisión operativa, permitiendo a los equipos de riesgo enfocarse en casos realmente relevantes.
- Optimización del tiempo de análisis, gracias a la inferencia acelerada por GPU.

NVDIA NIM-FRAUD BLUEPRINT: ARQUITECTURA SOLUCIÓN

El **Front/Back** Web en Next.js con Prisma permite que los usuarios registren y consulten datos de transacciones desde una interfaz moderna y rápida.

El **Coordinator**, desarrollado en FastAPI y desplegado en Docker, orquesta todo el flujo: recibe las solicitudes, consulta **MongoDB**, gestiona estados y decide cuándo enviar la información al para hacer inferencia.

La **base de datos** MongoDB almacena las transacciones, su clasificación y trazabilidad completa del proceso.



Triton Inference: sirrve como el motor de inferencia de alto desempeño, ejecutando el modelo de detección de fraude ya entrenado y devolviendo **el puntaje de fraude (fraud score)** para cada transacción.

Toda la solución corre sobre una **HPE L40S**, proporcionando la capacidad de GPU necesaria para servir el modelo de manera eficiente en tiempo real.

By COGNITIVA IA S.A.S

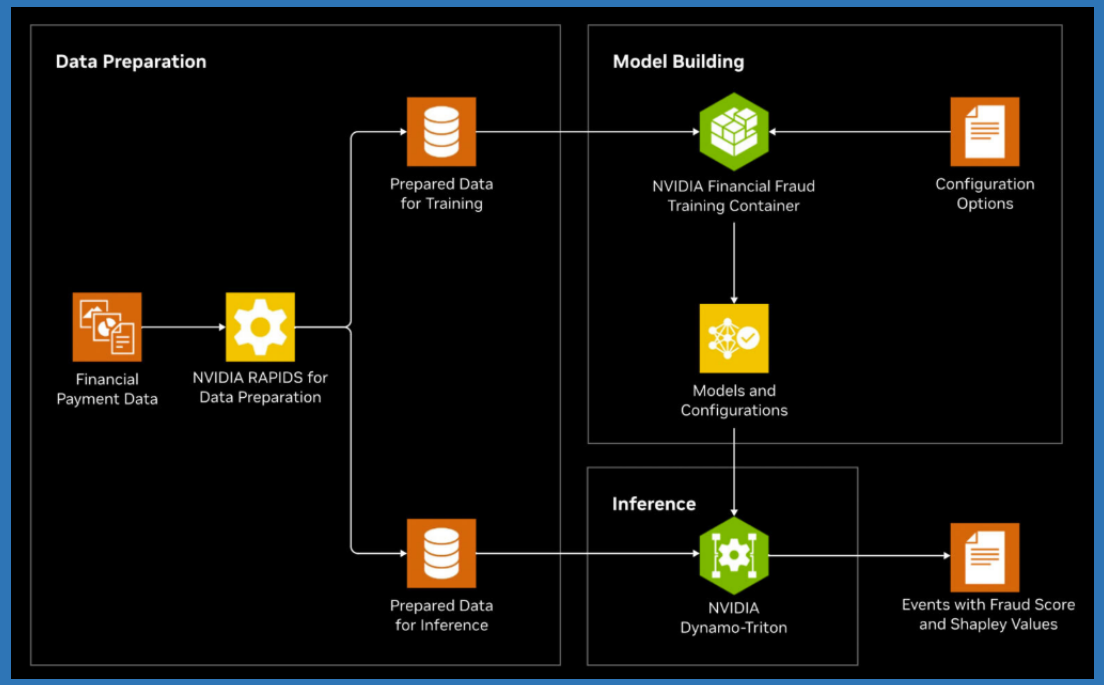
NVDIA NIM-FRAUD BLUEPRINT: ENTRENAMIENTO

1. Recepción de los datos preparados
Los datos transaccionales —ya limpiados, transformados y estructurados mediante RAPIDS— se envían al contenedor **NVIDIA Financial Fraud Training Container**, junto con las configuraciones definidas por el usuario (parámetros de entrenamiento, hiperparámetros, etc.).

2. Construcción del grafo transaccional
El contenedor se encarga internamente de:
- Tomar las transacciones financieras.
- Construir un **grafo** usando **cuGraph**, donde los nodos y conexiones representan relaciones entre clientes, tarjetas, comercios y operaciones.
- Esto permite capturar patrones complejos de fraude que los modelos tradicionales no detectan.

3. Entrenamiento del modelo GNN (Graph Neural Network)
Sobre ese grafo, el sistema entrena un modelo GNN cuyo objetivo es:
- **Aprender representaciones (embeddings)** de cada transacción.
- Capturar estructuras de comportamiento sospechoso en la red de relaciones.
- Estas representaciones contienen información muy rica sobre el contexto de cada operación.

4. Entrenamiento del modelo XGBoost
Una vez generados los embeddings, el contenedor:
- Utiliza esas representaciones como entrada para entrenar un modelo **XGBoost**.
- El objetivo final es **predecir el puntaje de fraude** de cada transacción.
- Esta combinación (GNN + XGBoost) ofrece gran precisión y menos falsos positivos.



HPE L40S

5. Generación de artefactos para inferencia
Al terminar el entrenamiento, el contenedor produce:
- El modelo final listo para producción.
- Los archivos de configuración.
- La estructura completa en un **NIM folder**.
- Estos artefactos deben entregarse al servidor **NVIDIA Dynamo-Triton**, donde se ejecutará la inferencia en tiempo real.

By COGNITIVA IA S.A.S

NVDIA NIM-FRAUD BLUEPRINT: DATA DE ENTRENAMIENTO

1. **Fuente de datos (IBM datSet):** https://ibm.ent.box.com/v/tabformer-data/folder/130747715605
2. **Total de registros: 24,386,900**
3. **Peso: 265 MB.**
4. **Variables independientes: 10**
5. **Variable dependiente: 1 (is Fraud?)**

	User	Card	Year	Month	Day	Time	Amount	Use Chip	Merchant Name	Merchant City	Merchant State	Zip	MCC	Errors?	Is Fraud?
0	1431	1	2012	11	24	14:19	$137.46	Swipe Transaction	-5920216026753360007	Garland	TX	75043.0	4111	NaN	No
1	368	0	2016	11	21	06:24	$162.71	Chip Transaction	3939208886321873731	Severn	MD	21144.0	5912	NaN	No
2	1462	0	2019	3	23	17:42	$26.55	Chip Transaction	6577593968895566254	Anaheim	CA	92805.0	5813	NaN	No
3	1618	0	2011	12	5	04:40	$17.10	Swipe Transaction	1913477460590765860	Blackwood	NJ	8012.0	5300	NaN	No
4	1158	1	2016	5	1	11:57	$77.00	Chip Transaction	-1288082279022882052	Aurora	CO	80013.0	5499	NaN	No
5	1110	0	2002	12	6	18:32	$51.18	Swipe Transaction	7069584154815291371	Miami	TX	79059.0	5812	NaN	No
6	1932	2	2015	10	2	12:00	$236.70	Online Transaction	-7162568984096711351	ONLINE	NaN	NaN	5733	NaN	Yes
7	1111	3	2009	9	14	03:47	$115.39	Online Transaction	-3220758452254689706	ONLINE	NaN	NaN	5311	NaN	Yes
8	545	1	2010	6	17	12:12	$6.39	Online Transaction	8376042053629658626	ONLINE	NaN	NaN	4131	NaN	Yes
9	576	1	2018	7	25	17:25	$3.83	Chip Transaction	7069584154815291371	Rome	Italy	NaN	5812	NaN	Yes

User
Identificador del usuario o cliente que realizó la transacción. No es el nombre real; es un ID anonimizado.

Card
Número interno que representa la tarjeta del usuario. Un usuario puede tener varias tarjetas.

Year / Month / Day / Time
Componentes de la fecha y hora de la transacción:
Year: año de la operación
Month: mes
Day: día
Time: hora exacta de la transacción

Zip
Código postal del comercio.

Use Chip
Método de transacción:
Swipe Transaction → banda magnética
Chip Transaction → chip EMV
Online Transaction → compra digital

Merchant State
Estado o región del comercio.
En compras online puede quedar vacío.

Merchant Name
Identificador del comercio o entidad donde se realizó la compra. Está anonimizado mediante números.

Errors?
Indica si hubo algún tipo de error asociado a la transacción.
En muchos datasets suele estar vacío o ser un campo técnico.

MCC (Merchant Category Code)
Código del tipo de comercio (por ejemplo, supermercados, gasolineras, comercio electrónico).
Es muy importante para análisis de fraude.

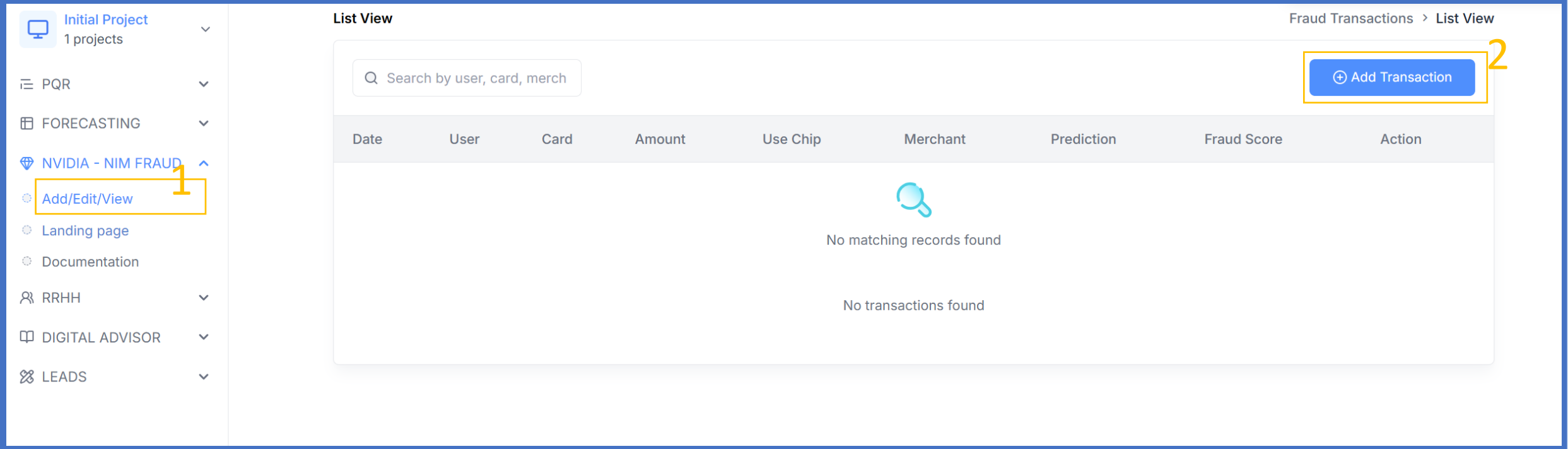
Is Fraud?
Variable objetivo (label):
Yes → transacción fraudulenta
No → transacción legítima
Es la columna que se utiliza para entrenar los modelos de detección de fraude.

Amount
Monto de la transacción. Puede incluir decimales y está expresado en dólares.

Merchant City
Ciudad donde está ubicado el comercio (si aplica).
Para transacciones en línea puede aparecer como **ONLINE**.

By COGNITIVA IA S.A.S

NVDIA NIM-FRAUD BLUEPRINT: PROCESO



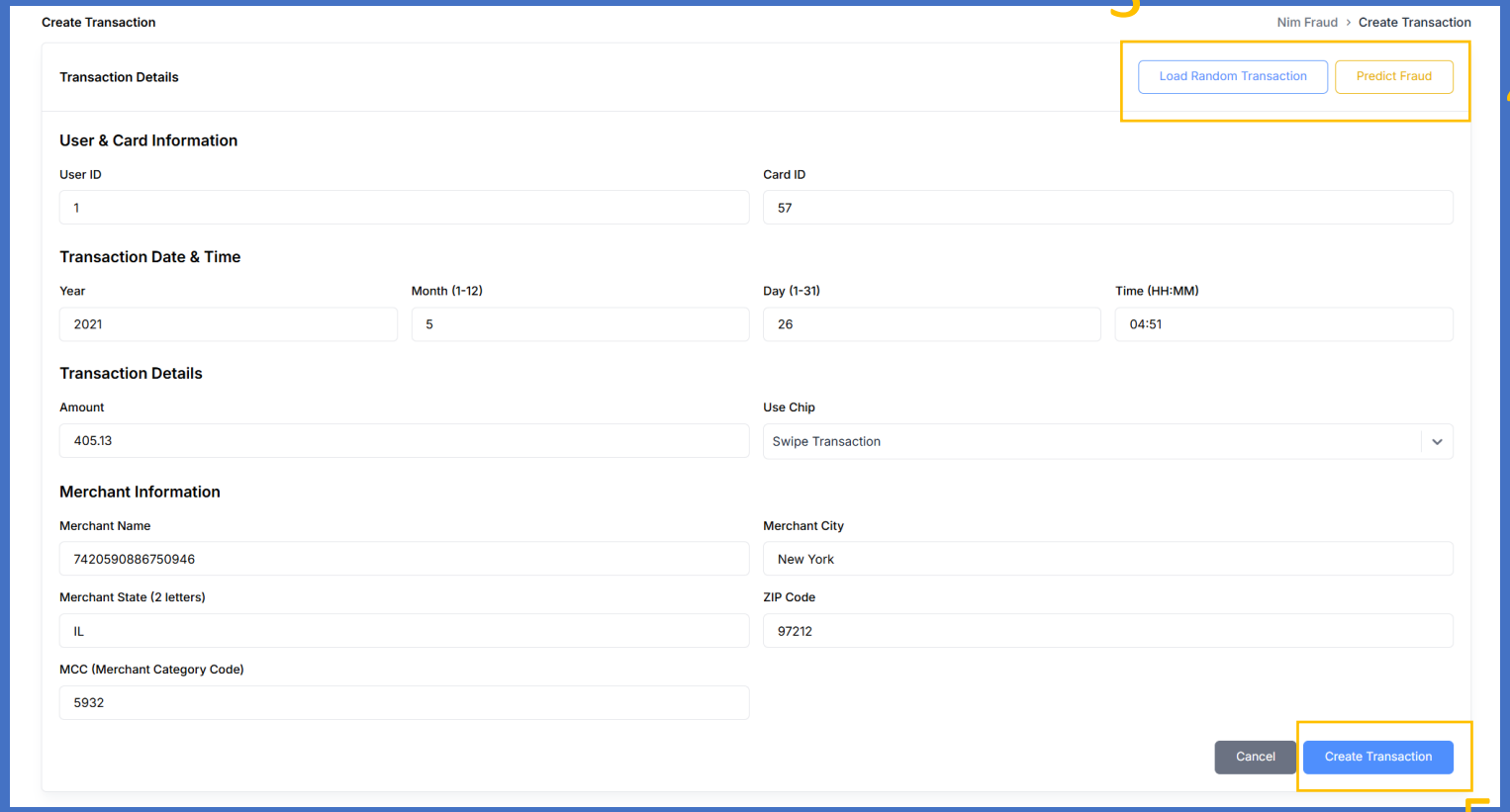
1 En el menú lateral izquierdo, haz clic en la opción **"Add/Edit/View"** dentro de la sección **NVIDIA – NIM FRAUD**.
Esta opción te permite acceder al módulo donde puedes agregar, editar o visualizar transacciones.

2 Una vez dentro del módulo de NVIDIA – NIM FRAUD, selecciona el botón **"Add Transaction"** ubicado en la parte superior derecha de la pantalla.

Al hacer clic, se abrirá el formulario para ingresar una Transacción para analizar..

NVDIA NIM-FRAUD BLUEPRINT: PROCESO

3



4

5

📝 Registro / Edición de una Transacción

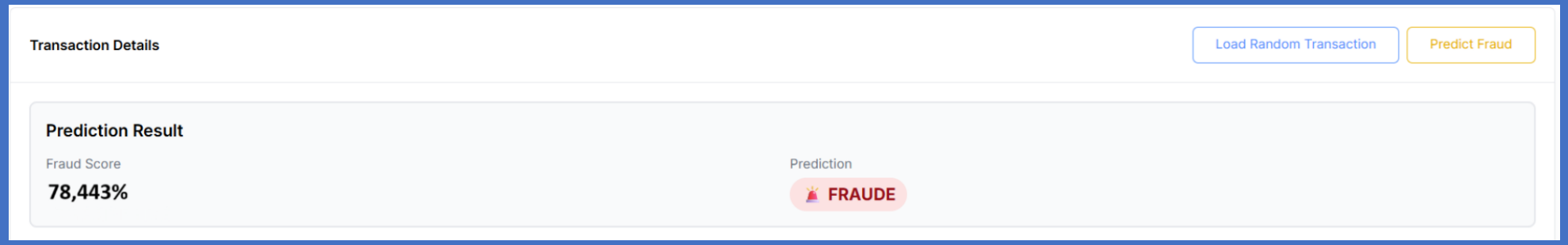
Puedes agregar manualmente los datos de una transacción.

O puedes pulsar el botón **Load Random Transaccion** para pre-llenar los campos.

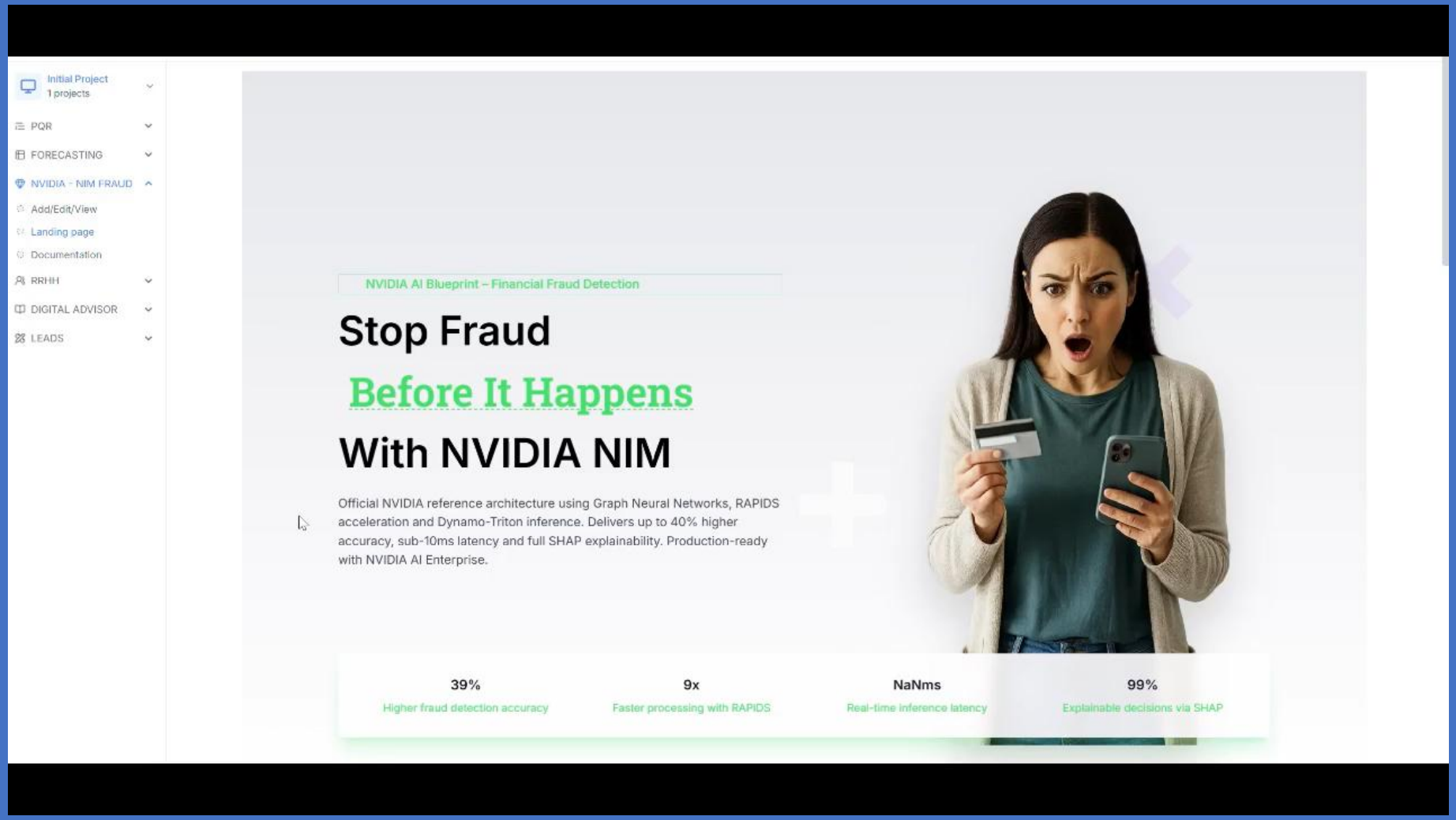
Una vez llenado los campos, hacer click en **Predict Fraud.**

Para finalizar puede Guardar la transacción en **Create Transaction.**

NVDIA NIM-FRAUD BLUEPRINT: PROCESO RESULTADO



🧠 **Resultado del análisis con IA**

El sistema evaluó la transacción seleccionada y generó un fraud score del 78,44%, lo que indica una alta probabilidad de que la operación sea fraudulenta según el modelo entrenado. Este puntaje se calcula combinando patrones detectados por la red neuronal de grafos (GNN) y el modelo XGBoost, los cuales analizan el comportamiento del usuario, las características del comercio y la estructura de relaciones entre transacciones. Dado que el valor supera el umbral definido por la institución, la plataforma clasifica la transacción como "FRAUDE", sugiriendo que debe ser bloqueada de inmediato o enviada a revisión prioritaria por el equipo de riesgo.

NVDIA NIM-FRAUD BLUEPRINT: PROCESO RESULTADO