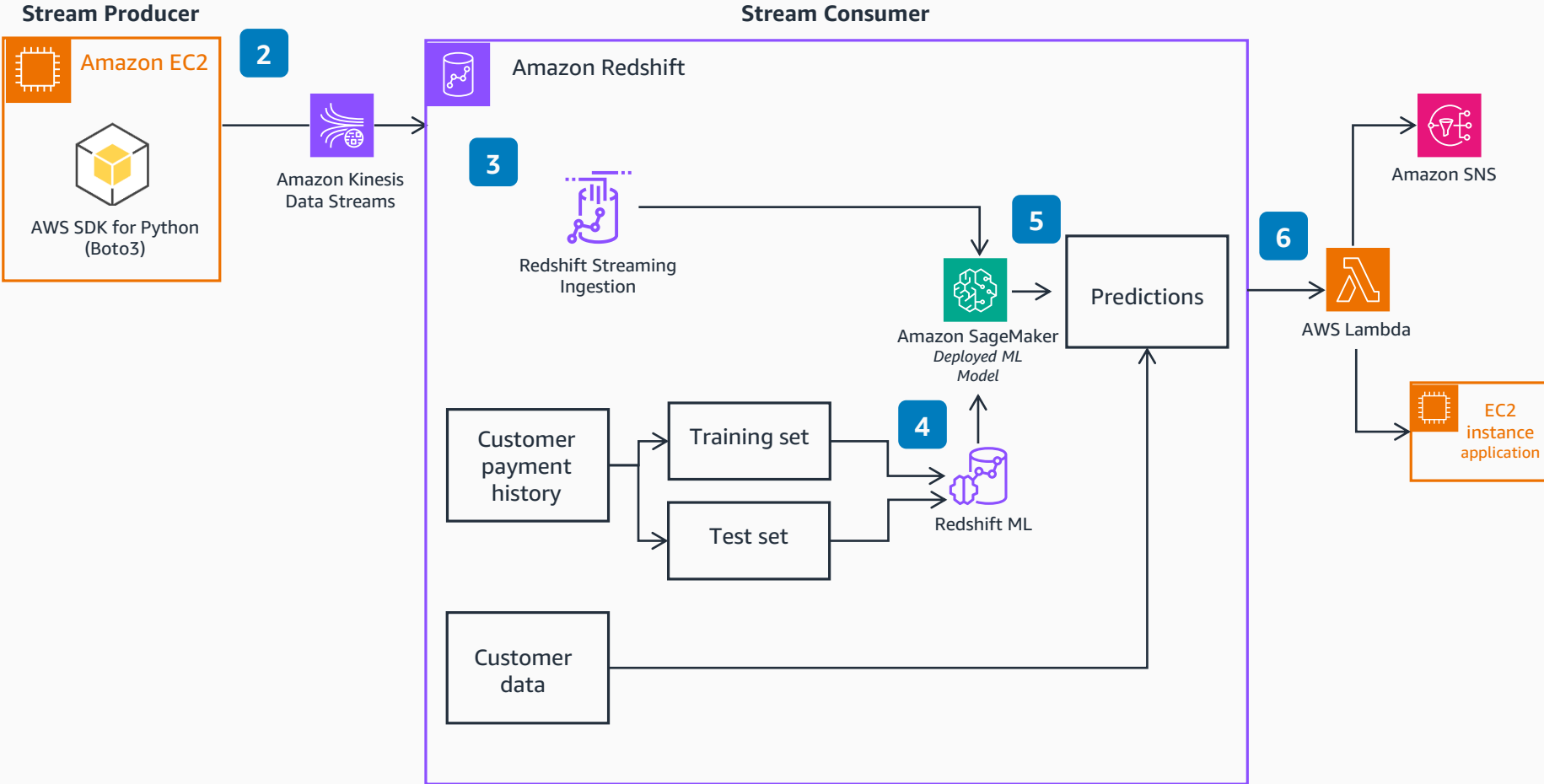


# Guidance for Near Real-Time Fraud Detection Using Amazon Redshift Streaming Ingestion

Use machine learning models trained on historical data to combat financial fraud in near real-time.

1



- 1 The **Amazon Elastic Compute Cloud** (Amazon EC2) instance simulates a credit card transaction application. It uses tools such as Python packages that generate fake data, and inserts credit card transactions into **Amazon Kinesis Data Streams**.
- 2 **Kinesis Data Streams** stores the incoming transaction data.
- 3 An Amazon Redshift Streaming Ingestion view is created on top of the data stream, which automatically ingests streaming data into **Amazon Redshift**.
- 4 Build, train, and deploy a machine learning (ML) model using Amazon Redshift ML. The Redshift ML model is trained using historical transactional data.
- 5 Generate ML predictions for the credit card transactions in the streaming data using **Amazon SageMaker**.
- 6 You can alert customers using **Amazon Simple Notification Service** (Amazon SNS). You can also update the **Amazon EC2** instance when you want to mitigate risk, such as blocking the financial transaction.