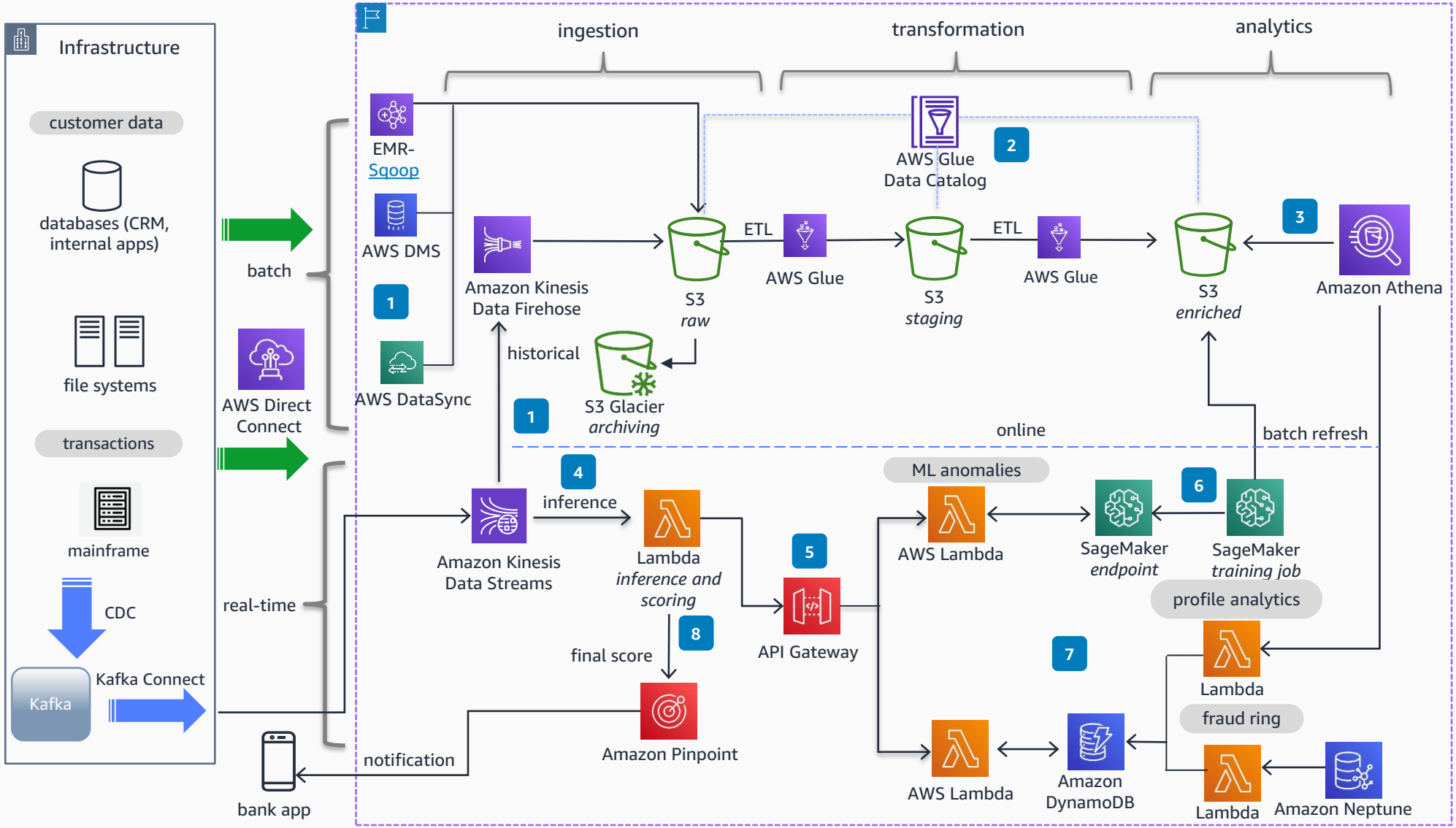
Guidance for Payments Fraud Prevention on AWS

This high-level reference architecture shows how payment companies can implement a near real-time fraud screening system on AWS



1. Large amounts of customer data stored in on-premises databases; file systems, and long-term historical data on mainframes is moved into **Amazon Simple Storage Service** (Amazon S3) using various data transfer services such as **Amazon EMR**, **AWS Data Migration Service** (AWS DMS), **AWS DataSync**, and **Amazon Kinesis Data Streams**.
2. Configure **AWS Glue** to initiate your extract, transform, load (ETL) jobs to run as soon as new data becomes available in Amazon S3.
3. **Amazon Athena** makes it easy to analyze data directly in Amazon S3 using standard SQL.
4. Near real-time transactions are sent to **Amazon Kinesis Data Streams**. **AWS Lambda** integrates natively with **Amazon Kinesis** as a consumer to process data ingested through a data stream.
5. Multiple **Lambda** functions is invoked from a single **Amazon API Gateway** for different kinds of inference.
6. An **Amazon SageMaker** notebook instance with different machine learning (ML) models that will be trained on the dataset gives a prediction score to the endpoint.
7. The fraud ring and profile analytics in near real-time that was queried through **Amazon Athena** is persisted in **Amazon DynamoDB**.
8. The final aggregated score is calculated based on inferences and a notification is sent to an end user in the event of fraud through **Amazon Pinpoint**.

Reviewed for technical accuracy November 15, 2022

AWS Reference Architecture