SUMMIT

TAIPEI

企業如何透過機器學習進行詐欺偵測
Introducing Amazon Fraud Detector: Detect more online fraud faster

Tim WU 武鯤鵬
Solutions Architect
Amazon Web Services

aws SUMMIT ONLINE

Current State of Fraud

Fraud can take many forms and impacts multiple industries

Globally each year, trillions of dollars are lost to online fraud. Companies conducting business online are especially prone to attacks from bad actors who often exploit different tactics such as creating fake accounts and making payments with stolen credit cards.

Examples of fraud

New Account

Guest Checkout

Loyalty/Incentive Abuse

Common industries impacted

Financial Services

E-commerce

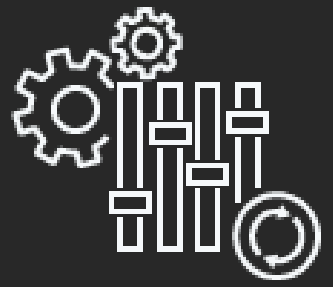
Travel and Hospitality

Fraudsters continually attack using different methods

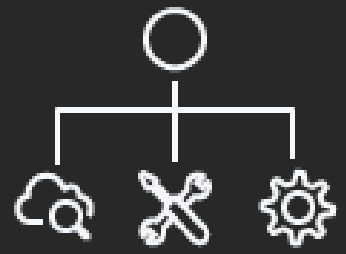
- Fraud has no consistent pattern user-to-user or domain-to-domain
- Constantly evolving threat environment: similar to security threats
- Must minimize cost of fraud vs. cost of losing annoyed customers
- Highly personalized

Fraud Prevention Strategy

Fraud detection is difficult



Bad actors change tactics often



Embedded detection logic

Costly human reviews

Fraud detection with ML is also difficult

Generic models underperform

Time-consuming data transforms

Needle in a haystack

Business Rules vs Machine Learning

Business Rules look for specific conditions or behaviors

- Business Rules are easily explained and validated
- Sample New Account Registration rule:

```
If IP_ADDRESS_LOCATION == ['Japan'] and CUST_ADDRESS_COUNTRY == ['JAPAN'] and CUSTOMER_PHONE_LOC == ['Spain'] THEN Investigate
```

ML Models learn more general patterns by looking at lots of examples

- When fraudsters make small tweaks, the model still recognizes them as suspicious since it's unlike anything it has seen from legitimate customers
- ML models are not just good at finding the risky patterns, they're much less brittle than rules

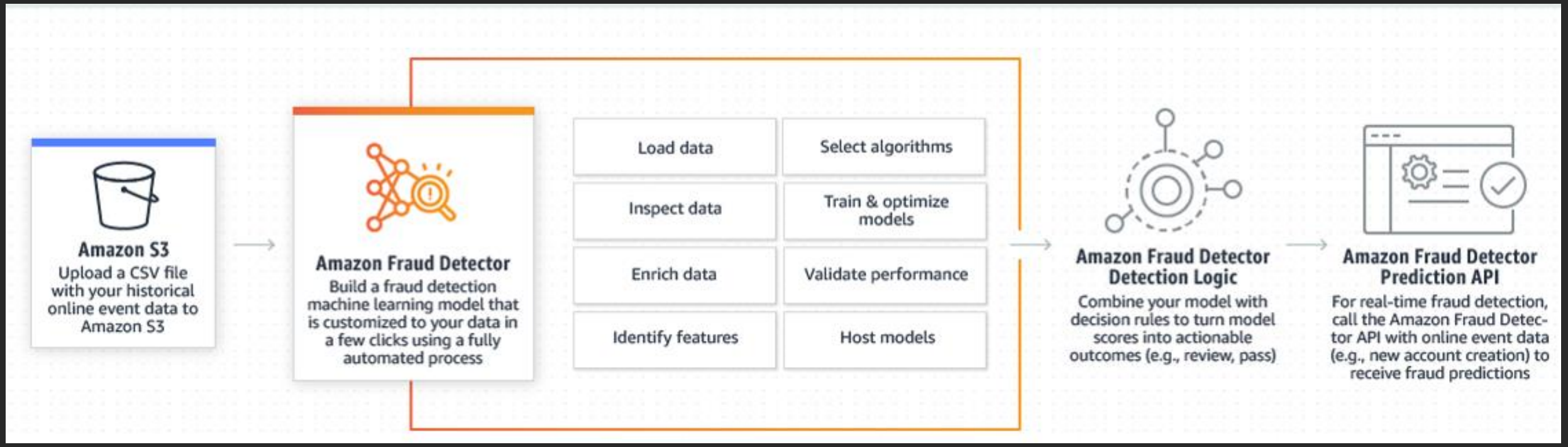
Machine learning-based fraud detection
The Amazon Approach

aws SUMMIT ONLINE

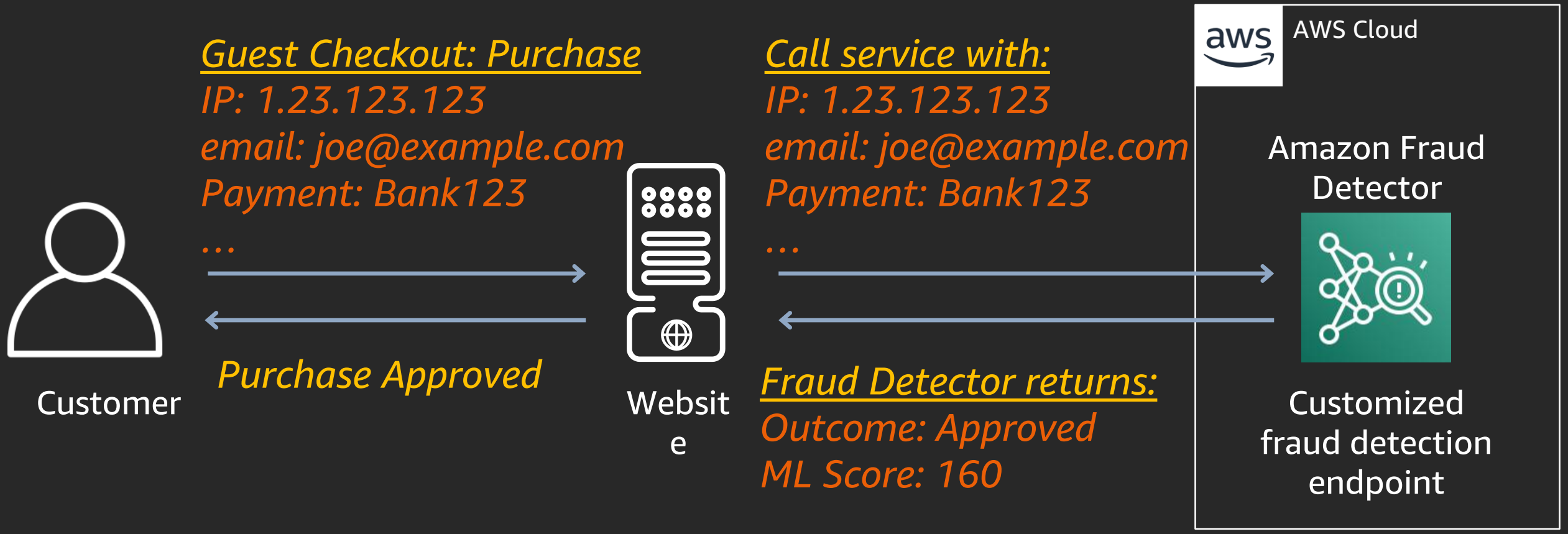
Introducing Amazon Fraud Detector

A fraud detection service that makes it easy for businesses to use machine learning to detect online fraud in real-time, at scale.

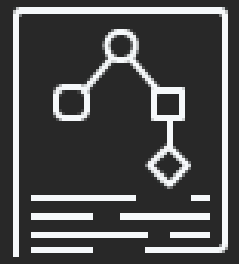
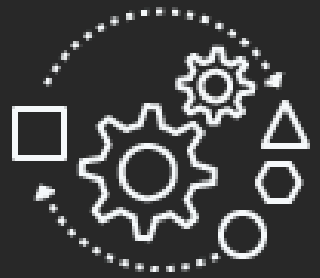
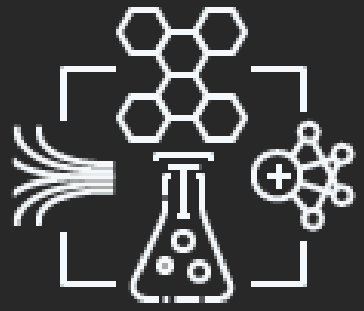
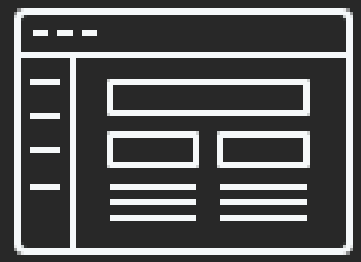
How it works


Amazon S3
Upload a CSV file with your historical online event data to Amazon S3
Amazon Fraud Detector
Build a fraud detection machine learning model that is customized to your data in a few clicks using a fully automated process
Load data
Select algorithms
Inspect data
Train & optimize models
Enrich data
Validate performance
Identify features
Host models
Amazon Fraud Detector Detection Logic
Combine your model with decision rules to turn model scores into actionable outcomes (e.g., review, pass)
Amazon Fraud Detector Prediction API
For real-time fraud detection, call the Amazon Fraud Detector API with online event data (e.g., new account creation) to receive fraud predictions

Generating Fraud Predictions



Key features

				
Pre-built fraud detection model templates	Automatic creation of custom fraud detection models	Models learn from past attempts to defraud Amazon	Amazon SageMaker integration	Interface to review past events and detection logic

Detect common types of online fraud

Designed to help companies detect common types of online fraud

Examples:

- New account fraud
- Guest checkout fraud
- ‘Try Before You Buy’ + post-paid online service abuse
- Online payment fraud (coming soon)
- Account takeover (coming soon)

Amazon Fraud Detector Benefits

- Detect risky events based on an event's attributes
- Best for detecting potential fraud when historical account/user data is limited
- Inspired by models and techniques used to protect AWS account registration
- Use cases: new account, first transaction, guest checkout
- Inputs: 3 required data elements and 50+ optional

Feedback from customers

Reaction from Re:Invent

"...Amazon Fraud Detector will be instrumental in identifying fraud patterns from our historical data as well as using Amazon's experience detecting fraud."

Kara Suro

VP, Fraud and Financial Crimes
Charles Schwab

Results from Amazon Fraud Detector preview customers

From Late Detection to Instant Prevention

- Situation: Large eCommerce/SaaS vendor experiencing online transaction attacks stemming from fake accounts
- Problem: Current fraud model identifies these accounts 10 days *after* account registration
- Solution: Amazon Fraud Detector accurately identifies fraudsters at the time of registration, stopping fraudsters before they can start

Rapid Deployment with Self-Service and Pre-Integration

- Situation: Payment services provider needs 24/7 fraud-based transaction monitoring
- Problem: Third party rules engines are too costly to operate and integrate with AWS services
- Solution Using Amazon Fraud Detector's self-service console and pre-integrations with Cloudwatch and CloudTrail, successfully built and deployed a model in 30 minutes then ramped up to production-level volume in a few weeks

Amazon Fraud Detector: Currently in preview

- Learn more
  - https://aws.amazon.com/fraud-detector/?nc2=type_a
- Try it out
  - https://pages.awscloud.com/amazon-fraud-detector-preview.html
- Resources
  - https://github.com/aws-samples/aws-fraud-detector-samples
  - https://aws.amazon.com/blogs/machine-learning/catching-fraud-faster-by-building-a-proof-of-concept-in-amazon-fraud-detector/

Thank you!

aws SUMMIT ONLINE