Flagging Payments for Fraud Detection: A Strategic Agent-Based Model

Katherine Mayo, Shaily Fozdar, and Michael P. Wellman

UNIVERSITY OF MICHIGAN

SRG Strategic Reasoning Group

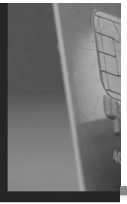
150+ Million Americans Victims of Credit Card Fraud Up from 127 Million a Year Ago, According to New Security.org Annual Research

Security.org
Tue, January 31, 2023 at 10:30 AM EST · 1 min read

NEWPORT NEWS

Newport News police warn of credit card scam at local 7-Eleven

/ 04:02 PM EST
3 / 08:40 AM EST



FOR IMMEDIATE RELEASE Tuesday, January 17, 2023

Bronx Man Admits Role in Nationwide Credit Card Fraud Affecting Thousands of Account Holders

NEWARK, N.J. – A manager for a conspiracy that used stolen credit card information to make fraudulent retail purchases around the United States pleaded guilty today, U.S. Attorney Philip R. Sellinger announced.

Trevor Osagie, 31, of the Bronx, New York, pleaded guilty before U.S. District Judge William Martini in Newark

LOCAL

Don't get scammed with credit card skimmers: How to avoid theft at gas stations

Springfield Police Department warns of increases in scam and credit card fraud

Credit card fraud is a notorious issue that is only growing.

Thornhill man charged in $36,000 credit card fraud case

+ PREFERRED REGION Durham | Crime | Latest News

By Liam McConnell
Published January 18, 2023 at 3:56 pm

Tech Layoffs: Shocking Story of a Former Google Employee Fired for Credit Card Fraud Amidst Mass Layoff

Tech Layoffs: Google, Amazon, Meta, Microsoft, and many more Tech firms are laying off people, while the stories of people being fired is extremely sad, one person has been disguising her firing from Google for fraud behind the seasonal layoffs. Here is the full story.

Authored by: TN Tech Desk | Updated Feb 4, 2023 | 05:54 PM IST

Wallet theft quickly turns into $6,000 credit card fraud: Mayfield Heights Police Blotter

Updated: Jan. 23, 2023, 8:11 p.m. | Published: Jan. 23, 2023, 7:35 p.m.

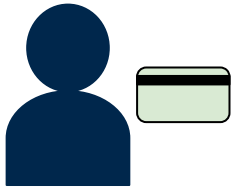
Video Game-Playing Fish Commit Credit Card Fraud In the Ultimate Phishing Scam

A good reminder to maybe not have your login and credit card info saved everywhere.

By Andrew Liszewski | Published January 20, 2023 | Comments (13)

Background: Credit Card Fraud

- A malicious actor obtains a customer's credit card details and uses it to make unauthorized purchases



Background: Credit Card Fraud

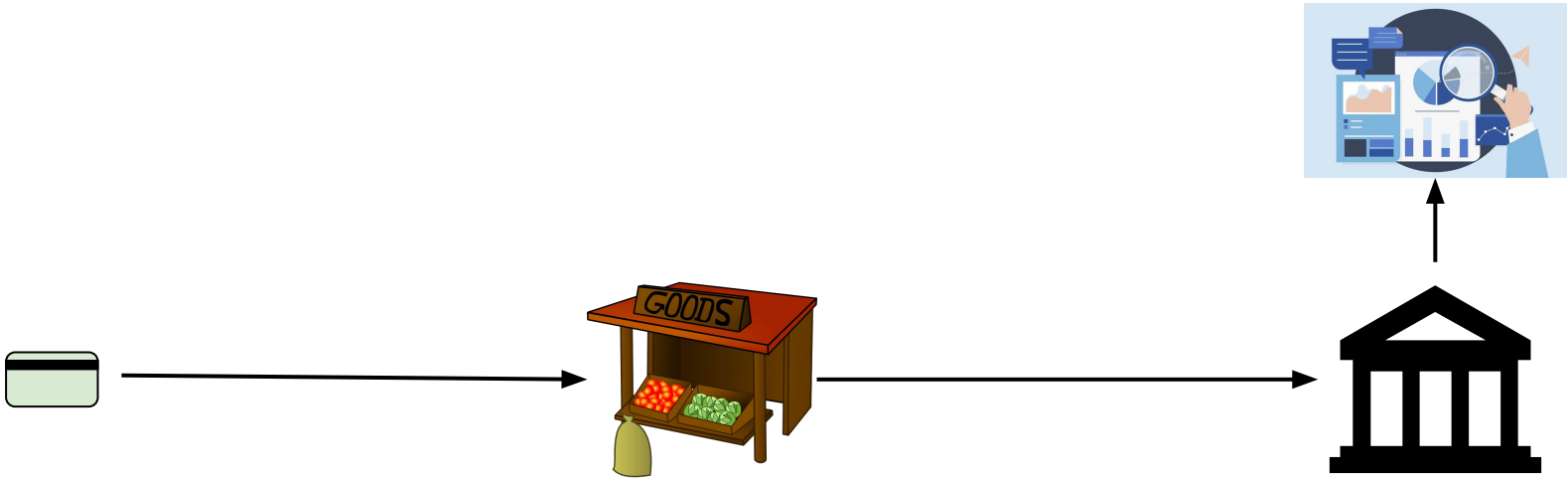
- A malicious actor obtains a customer's credit card details and uses it to make unauthorized purchases

Background: Fraud Detection

- A system for detecting whether a payment is fraudulent or non-fraudulent

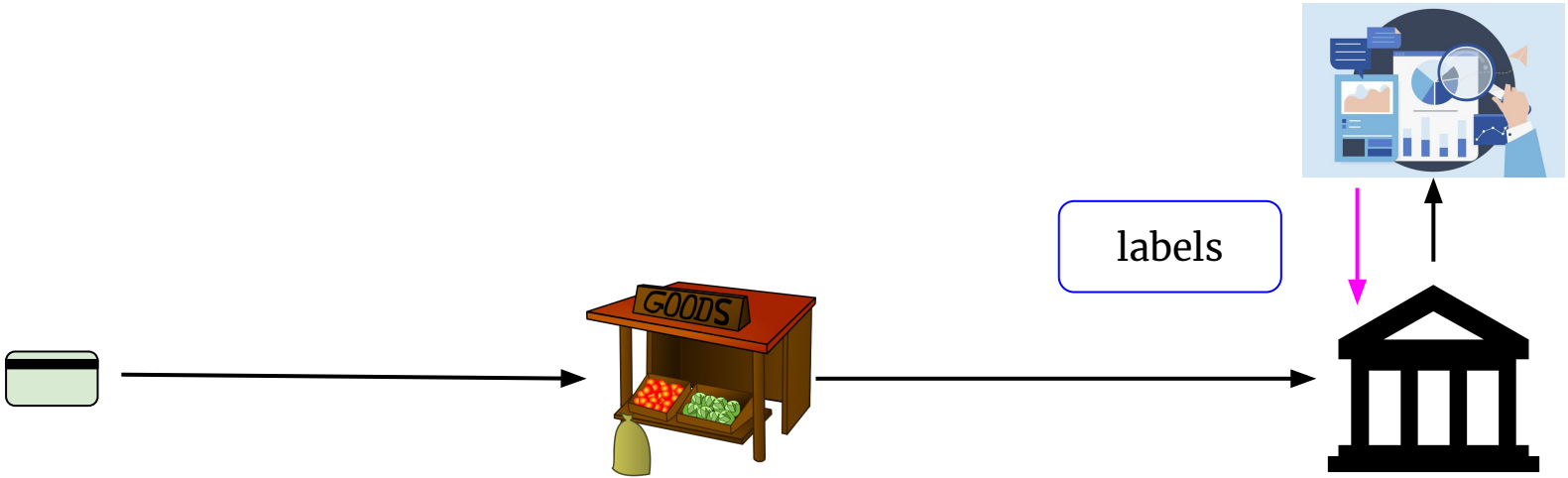
Background: Fraud Detection

- A system for detecting whether a payment is fraudulent or non-fraudulent



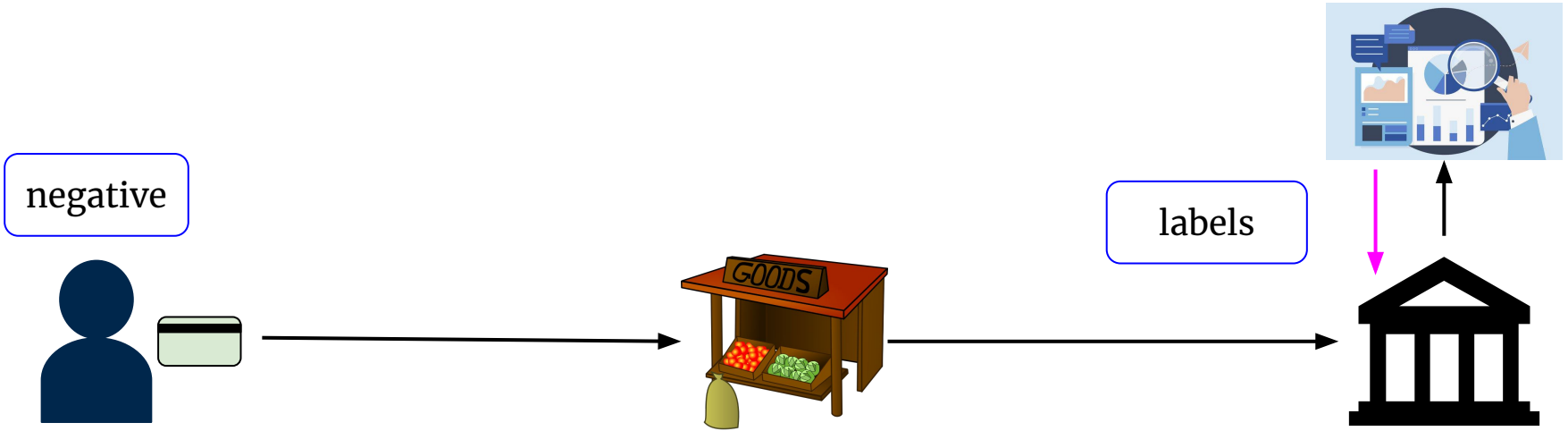
Background: Fraud Detection

- A system for detecting whether a payment is fraudulent or non-fraudulent



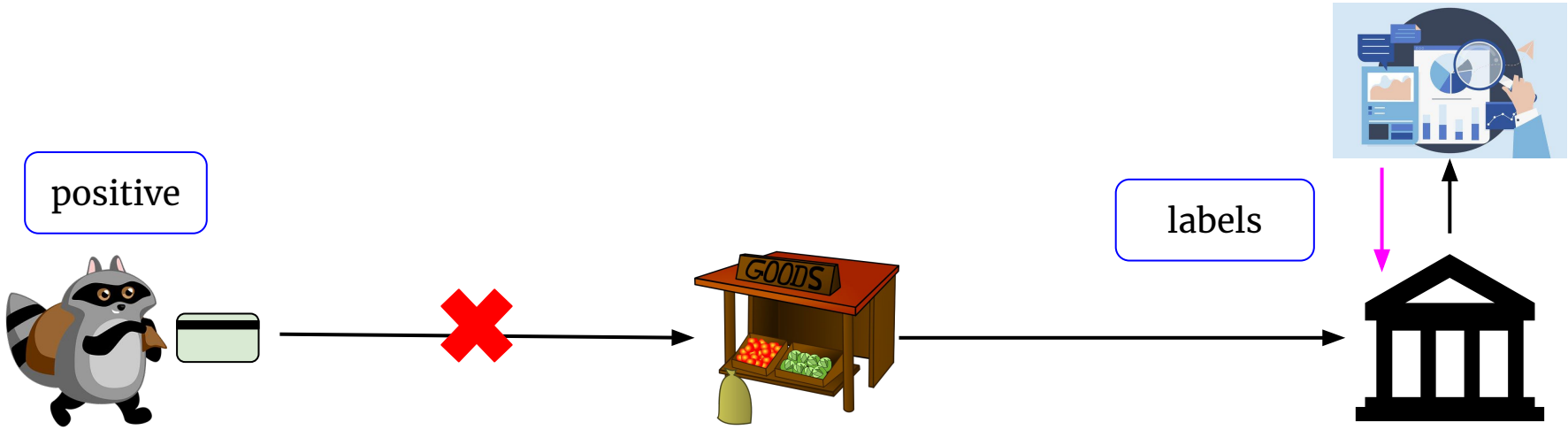
Background: Fraud Detection

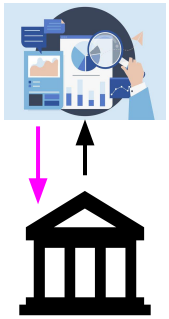
- A system for detecting whether a payment is fraudulent or non-fraudulent



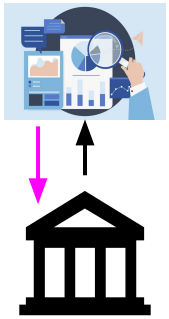
Background: Fraud Detection

- A system for detecting whether a payment is fraudulent or non-fraudulent





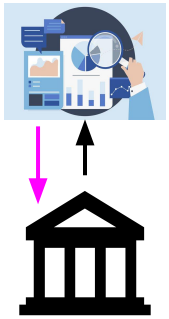
Fraud detection comes at a cost



Fraud detection comes at a cost

Payment

- Resources for analysis
- False positives (lost transaction fees)
- ...



Fraud detection comes at a cost

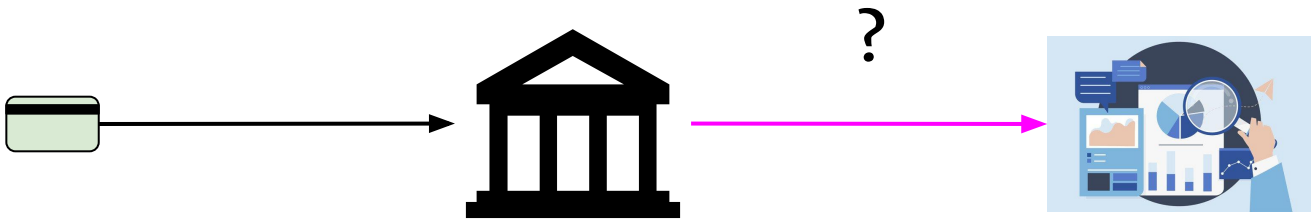
Payment

- Resources for analysis
- False positives (lost transaction fees)
- ...

Customer Disruption

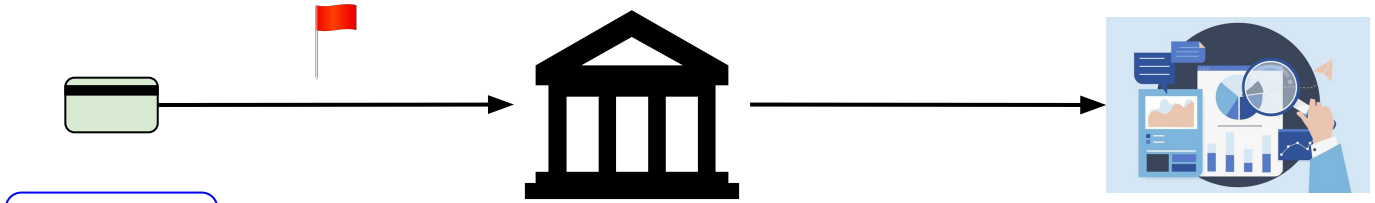
- Time for review
- False positives (lost business)
- ...

Fraud detection comes at a cost



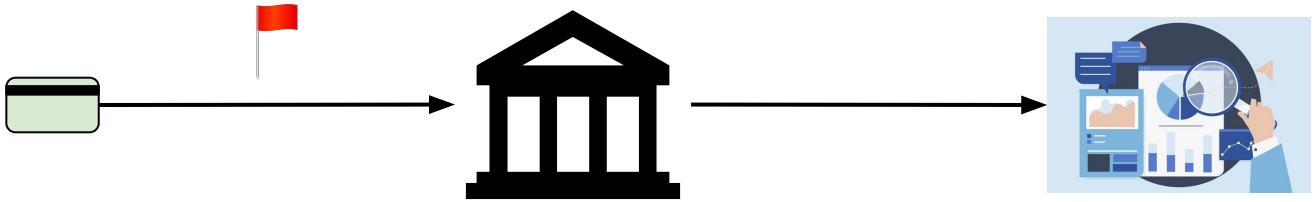
Banks may choose to be *strategic* about which payments are sent for fraud detection.

Fraud detection comes at a cost



flagging

Fraud detection comes at a cost

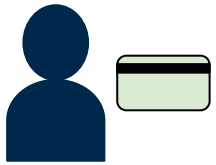


Flagging problem: Which payments should be *flagged* for review?

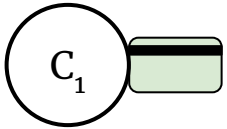
We explore strategic use of fraud detection by analyzing the **flagging problem** as a flagging game played by nodes in a payment network.

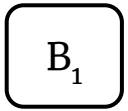
We explore strategic use of fraud detection by analyzing the **flagging problem** as a flagging game played by nodes in a payment network.

Payment Network: Modeling Credit



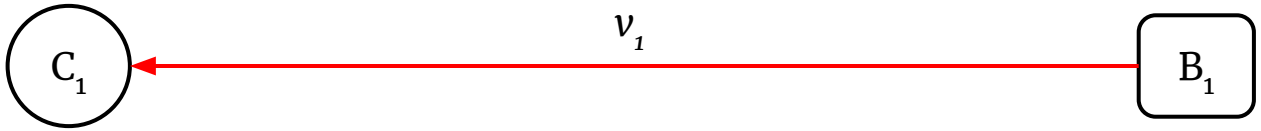
Payment Network: Modeling Credit





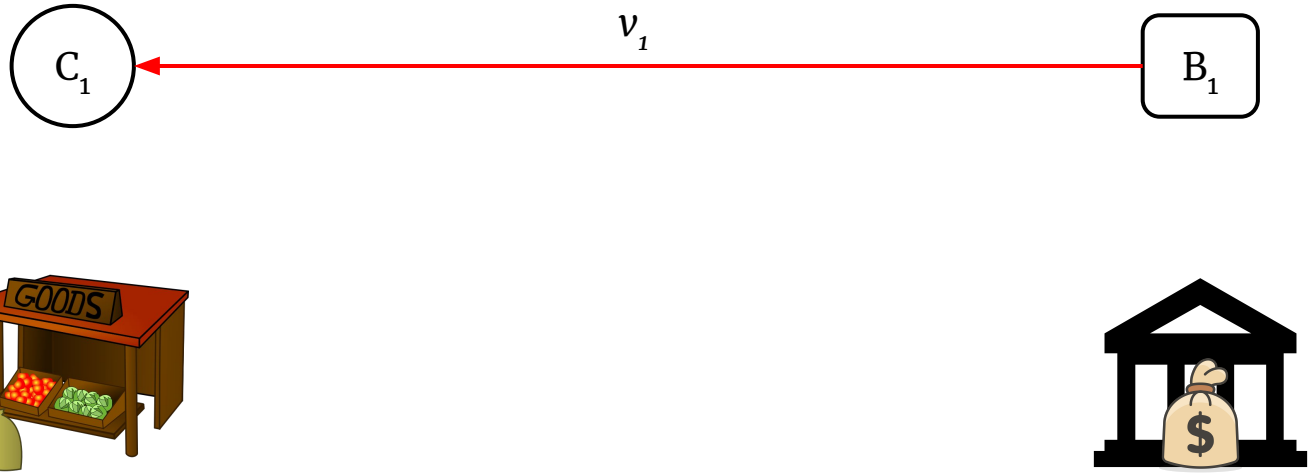
credit

Payment Network: Modeling Credit



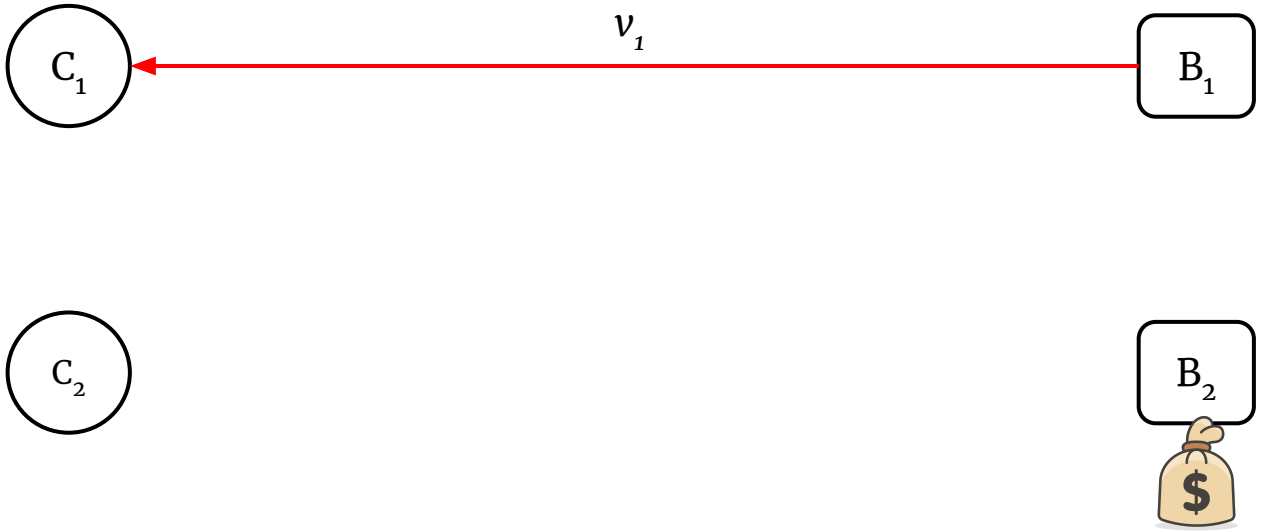
credit

Payment Network: Modeling Deposits

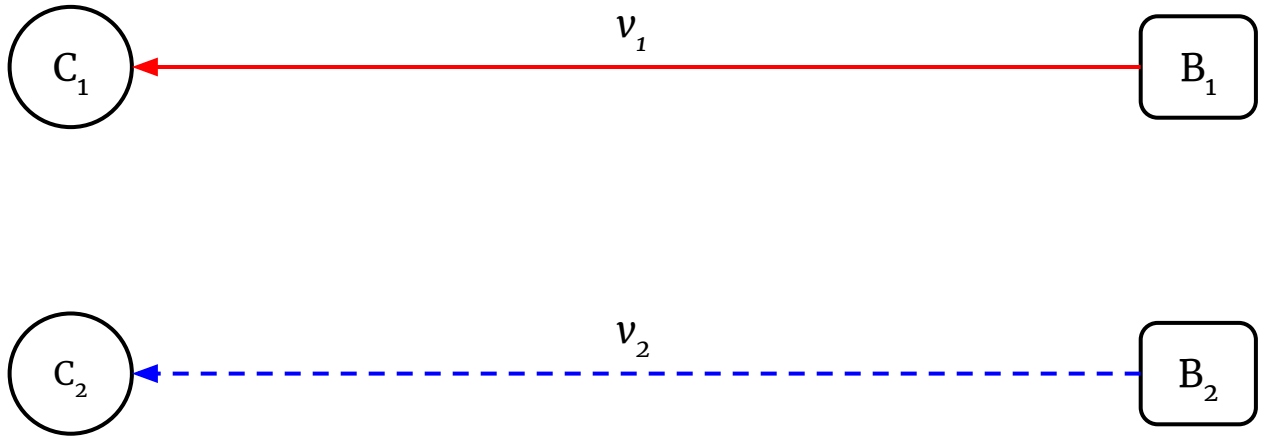


credit

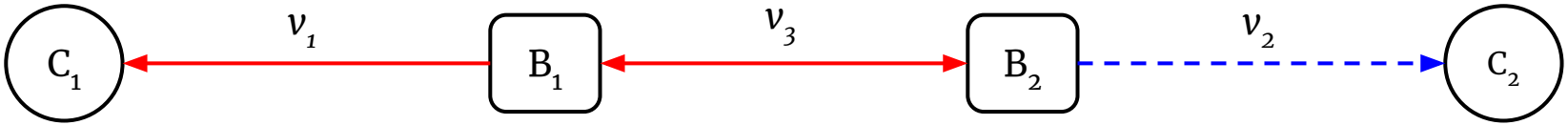
Payment Network: Modeling Deposits



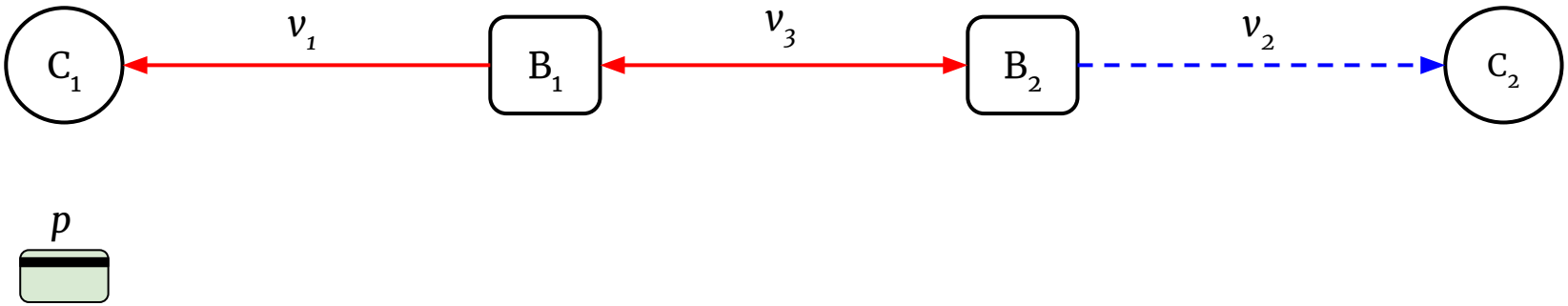
Payment Network: Modeling Deposits



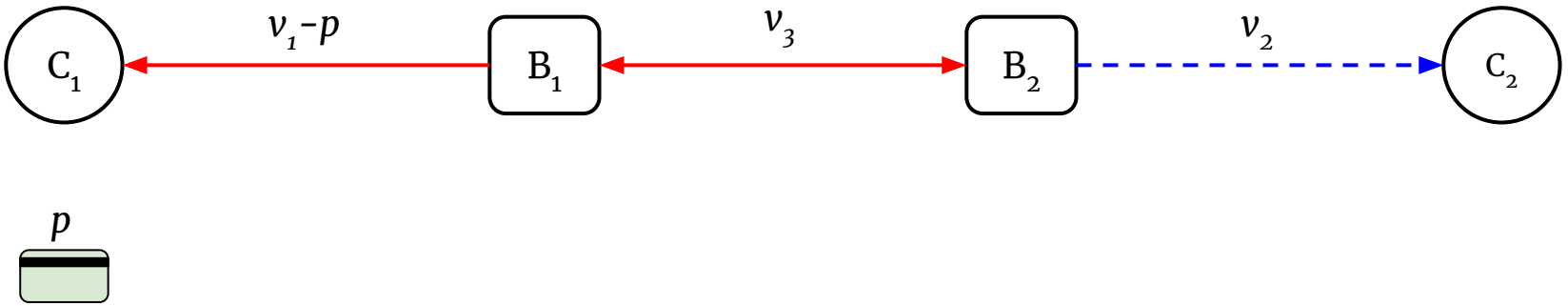
Payment Network: Modeling Payments



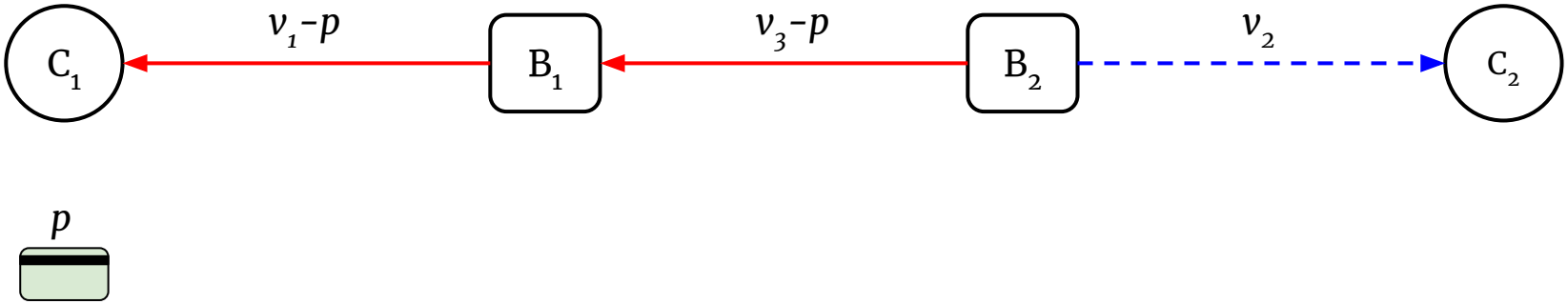
Payment Network: Modeling Payments



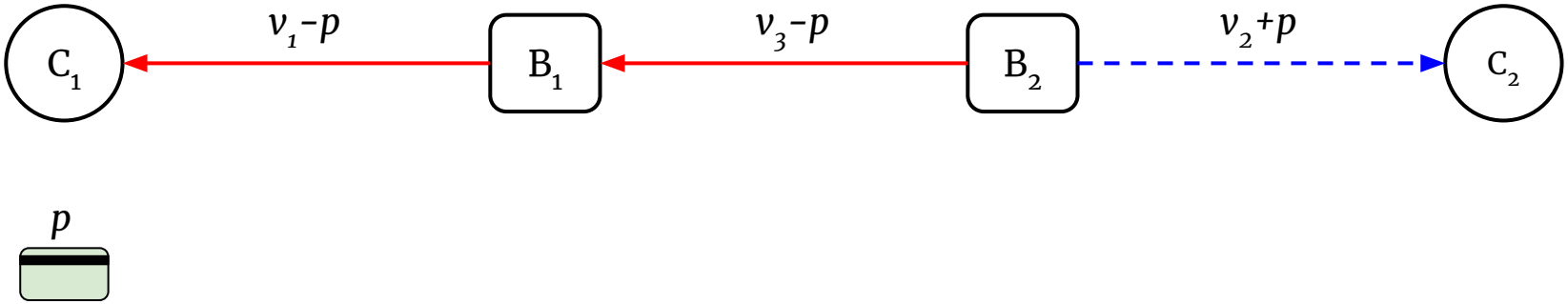
Payment Network: Modeling Payments



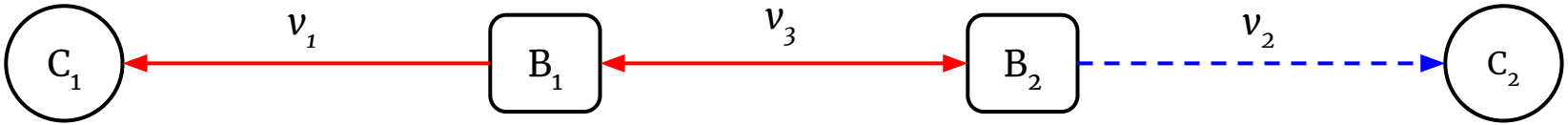
Payment Network: Modeling Payments

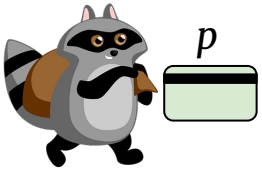


Payment Network: Modeling Payments

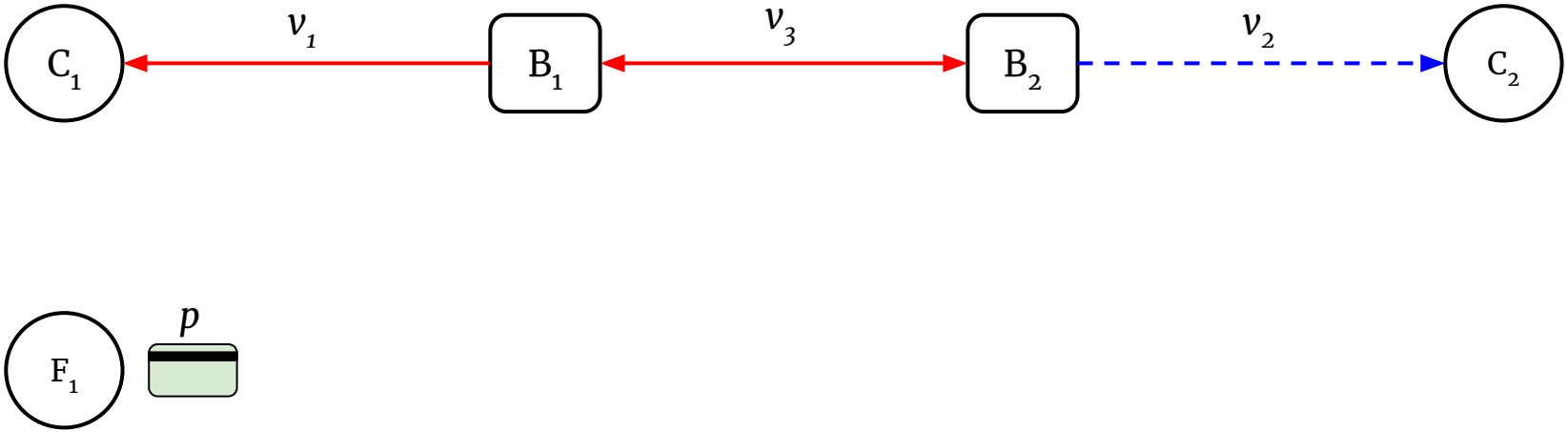


Payment Network: Modeling Fraud

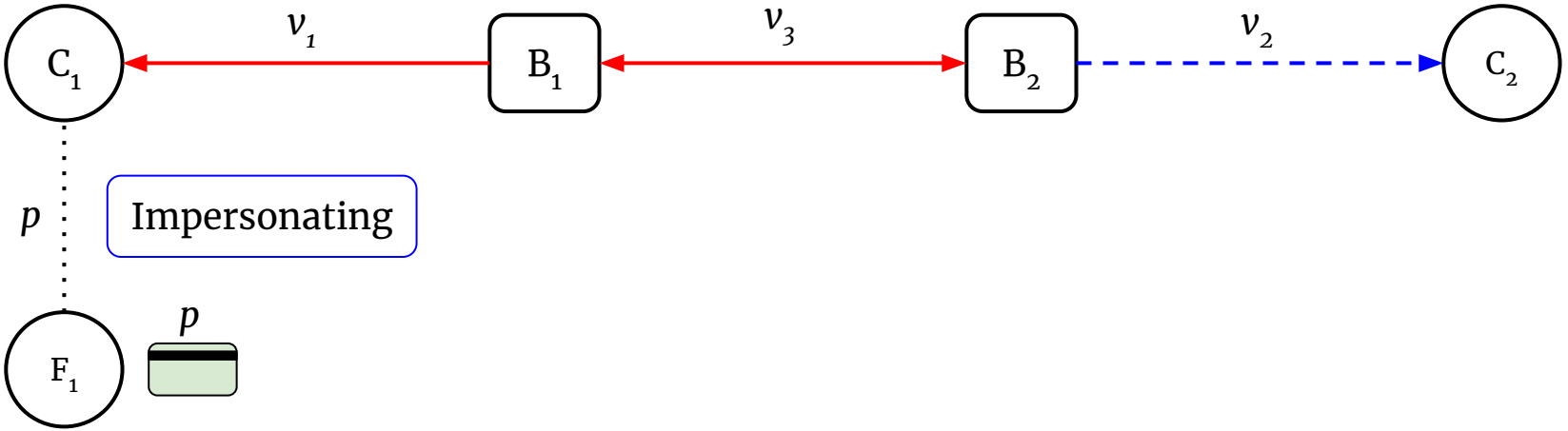




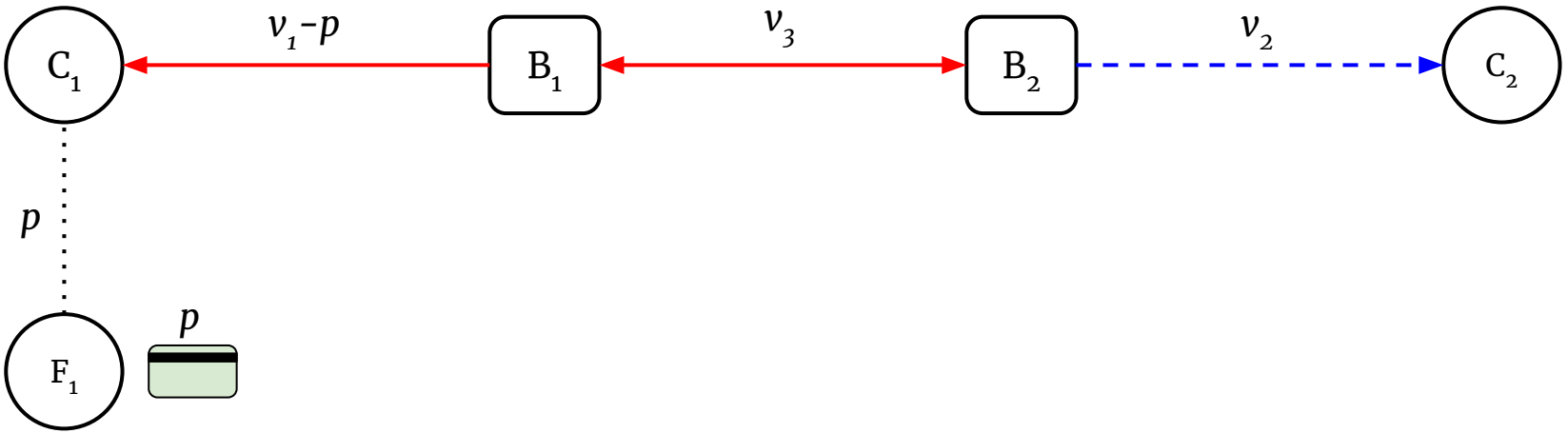
Payment Network: Modeling Fraud



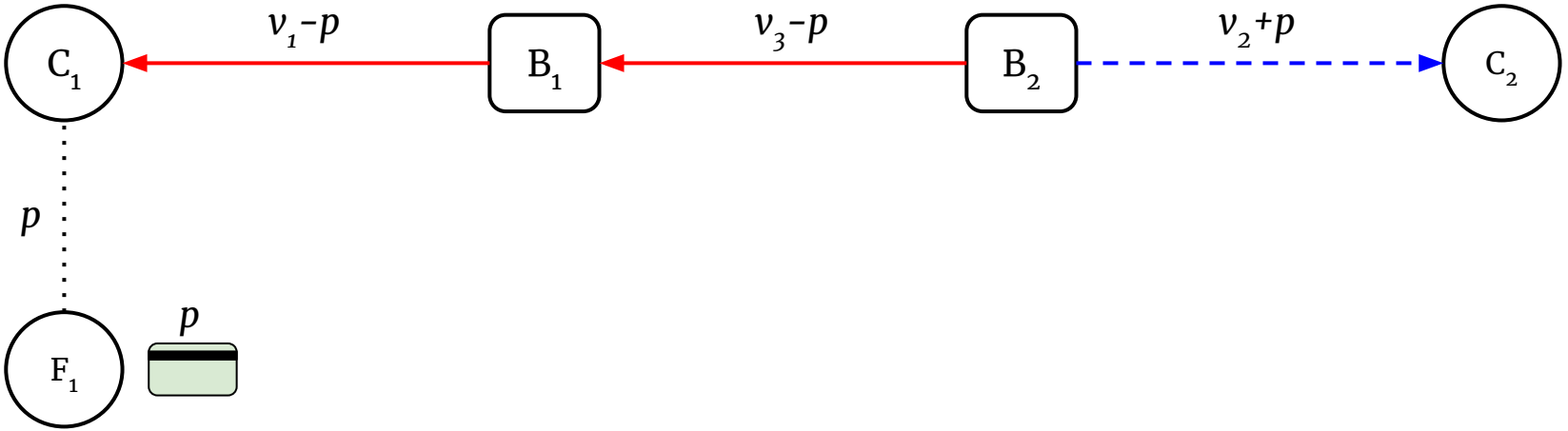
Payment Network: Modeling Fraud

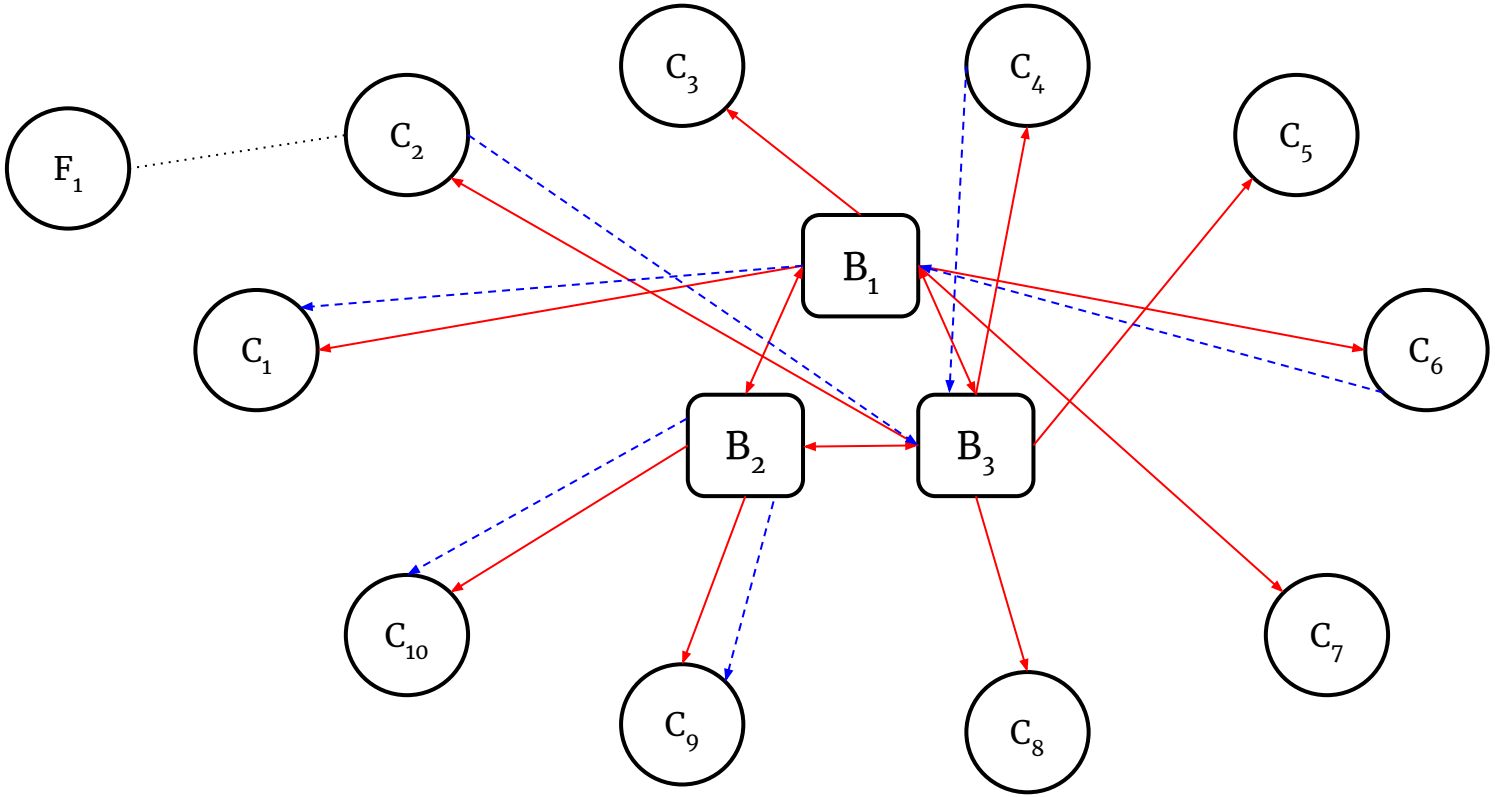


Payment Network: Modeling Fraud



Payment Network: Modeling Fraud




F1
C2
C3
C4
C5
B1
C1
C6
B2
B3
C10
C9
C8
C7

We explore strategic use of fraud detection by analyzing the **flagging problem** as a flagging game played by nodes in a payment network.

Flagging Payments Game Overview

- Background agents
- Behavior is dictated by JP Morgan synthetic data set

Flagging Payments Game Overview

- Background agents
- Behavior is dictated by JP Morgan synthetic data set

- Black box fraud detection system
- Characterized by probability correctly labels payment relative to its true label
    - Strong (high probability) banks and weak banks

Flagging Payments Game Overview

- Background agents
- Behavior is dictated by JP Morgan synthetic data set

- Black box fraud detection system
- Characterized by probability correctly labels payment relative to its true label
  - Strong (high probability) banks and weak banks

- Strategically selects customers to impersonate in a manner that targets banks where it is more likely to be successful
- Continue impersonating a customer until a payment attempt is blocked

Flagging Payments Game Overview

- Black box fraud detection system
- Characterized by probability correctly labels payment relative to its true label
  - Strong (high probability) banks and weak banks

- Strategically selects customers to impersonate in a manner that targets banks where it is more likely to be successful
- Continue impersonating a customer until a payment attempt is blocked

Flagging Payments Game Overview

	Banks	Fraudsters
Strategies	Determines the probability a payment is flagged for detection • Based on various attributes of the payment • Logistic functions • 12 total strategies	
Payoff	• Cost of undetected fraud • Cost of false positives • Cost of resources for detection	

Flagging Payments Game Overview

	Banks	Fraudsters
Strategies	Determines the probability a payment is flagged for detection • Based on various attributes of the payment • Logistic functions • 12 total strategies	Determines the value and frequency of payments • 8 total strategies
Payoff	• Cost of undetected fraud • Cost of false positives • Cost of resources for detection	• Value of undetected fraud

Analyzing the Flagging Game

- Network configuration
  - 4 banks: 2 strong, 2 weak
  - 1 fraudster
  - 200 customers
- Various game configurations defined by detection costs
  - Cost of false positives
  - Cost of fraud detection
- Employ empirical game-theoretic analysis (EGTA) to analyze the game
  - Uses extensive simulation of strategy profiles
  - Goal: identify Nash equilibria

Flagging Game Equilibria

	Fraudster	Weak Banks	Strong Banks
Low Detection Costs	Frequent payment attempts of high value		
High Detection Costs			

Flagging Game Equilibria

	Fraudster	Weak Banks	Strong Banks
Low Detection Costs	Frequent payment attempts of high value	High probability of flagging any given payment	High probability of flagging any given payment
High Detection Costs			

Flagging Game Equilibria

	Fraudster	Weak Banks	Strong Banks
Low Detection Costs	Frequent payment attempts of high value	High probability of flagging any given payment	High probability of flagging any given payment
High Detection Costs	Frequent payment attempts of high value	High probability of flagging any given payment	High probability of flagging payments with multiple suspicious attributes *only*

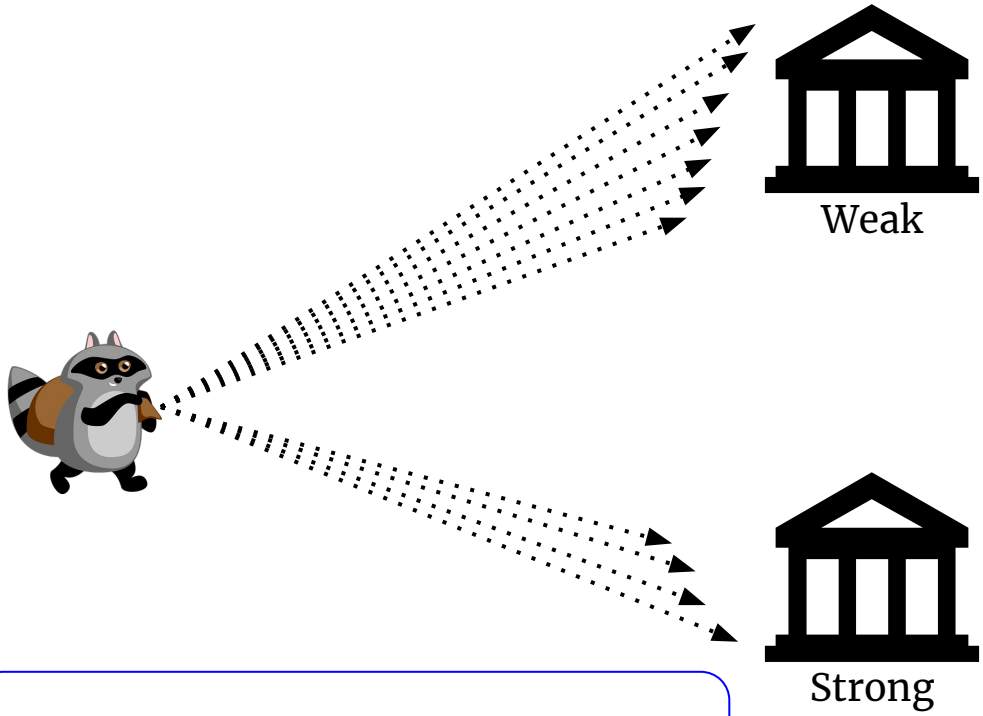
Intuition

Weak

Strong

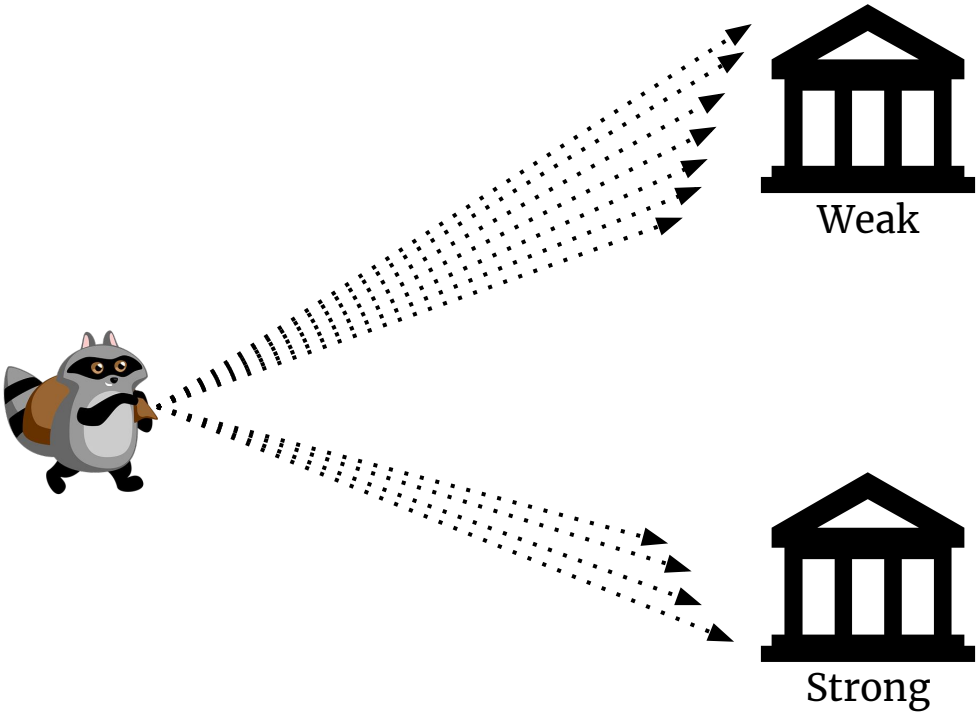
Recall: fraudsters target banks where they are more likely to be successful.

Intuition

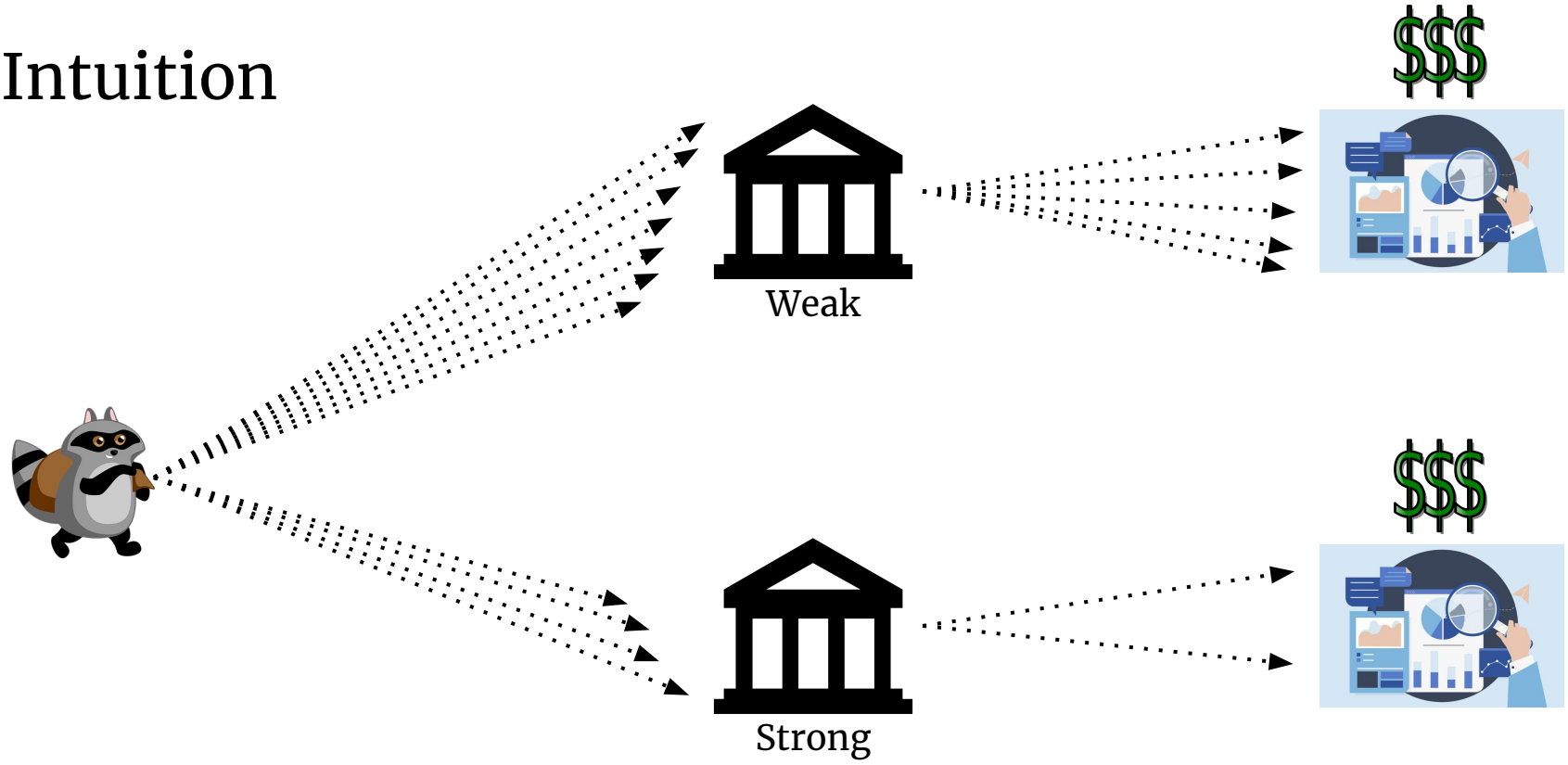


Recall: fraudsters target banks where they are more likely to be successful.

Intuition



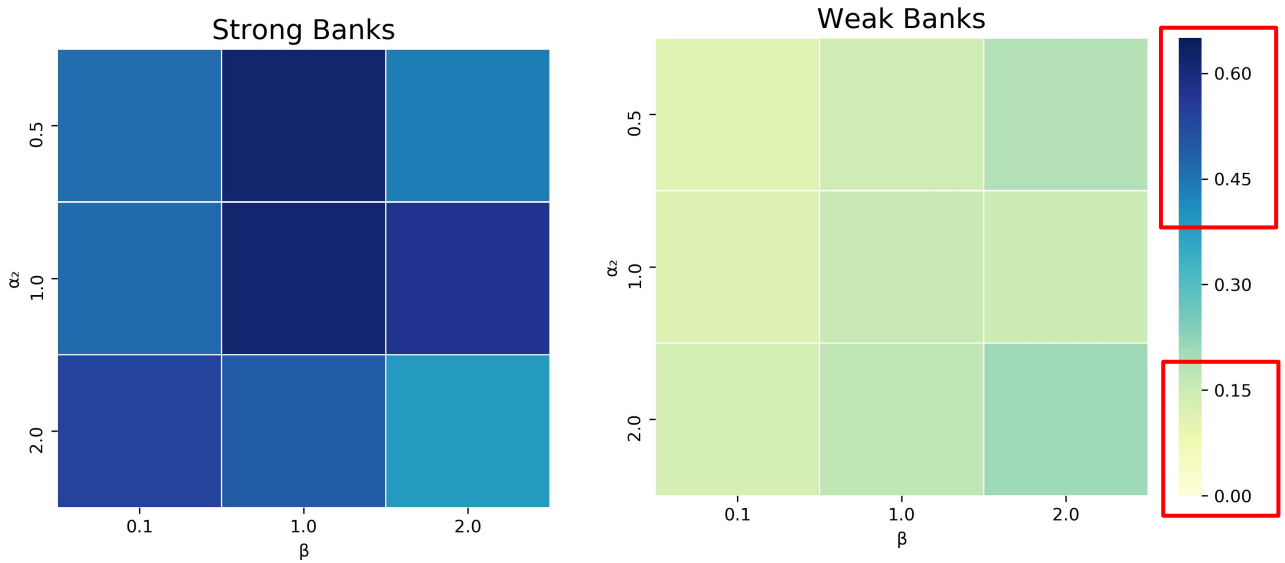
Intuition



With fewer attempted fraudulent payments, strong banks are able to make a trade-off between costs of missing fraudulent payments and costs of detection.

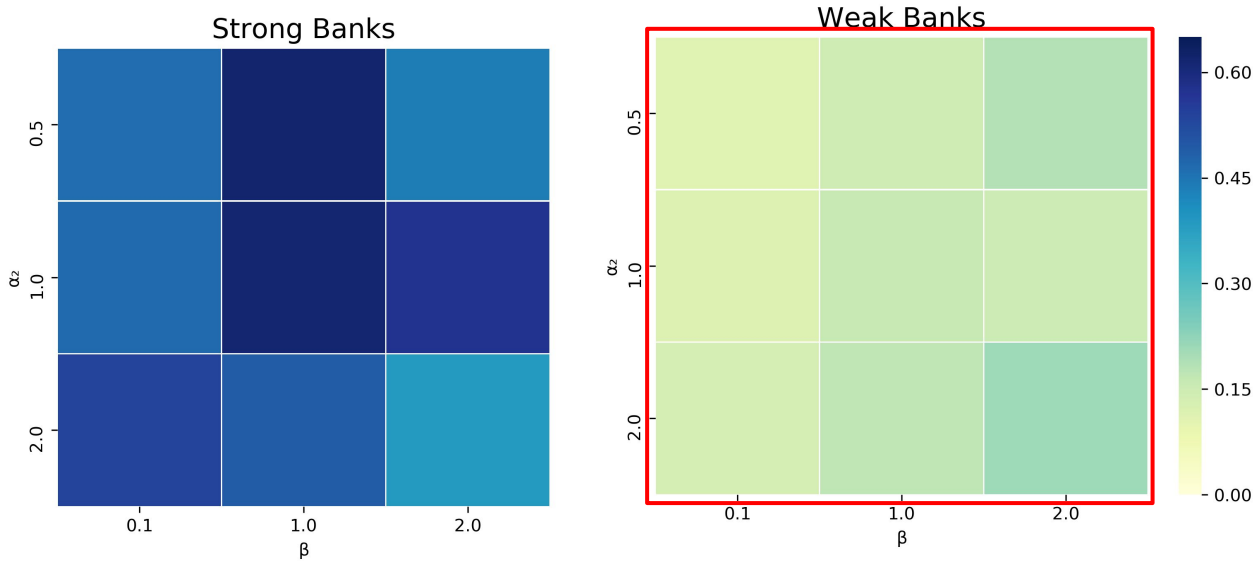
Proportion of Total Costs Attributed to Fraud Detection Costs

Proportion of Total Costs Attributed to Fraud Detection Costs



The cost of fraud detection is a larger proportion of total costs for strong banks explaining why increasing costs may affect the strategy of strong banks.

Proportion of Total Costs Attributed to Fraud Detection Costs



Even at high costs, the dominant cost for weak banks is fraudulent payments helping to explain why they do not change their strategy.

Main Takeaways

- Strong banks are more selective with fraud detection when associated costs are high
- Demonstrates the importance of considering other players' capabilities in the decision
  - Strong banks depend on the existence of weak banks

- Suggests similar fraud-related decisions may also exhibit strategic interdependencies
  - Ex: changing investment in a detection system

Thank you

Paper

https://kmayo.com/research.html

Additional questions/comments:
kamayo@umich.edu