BOXER: Preventing fraud by scanning credit cards

Zainul Abi Din, Hari Venugopalan, Jaime Park, Andy Li, Weisu Yin, Haohui Mai,
Yong Jae Lee, Steven Liu and Samuel T. King

UC DAVIS
UNIVERSITY OF CALIFORNIA

Bouncer

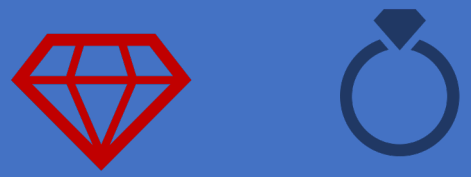
Once upon a time in 2018

Image from “Donnie Brasco, 1997”

Image from “Donnie Brasco, 1997”

Hey, I want to be Don the jeweler

Image from “Donnie Brasco, 1997”



I don’t know anything about GEMS

Get a PhD in Gemology?

GG

GRADUATE GEMOLOGIST® PROGRAM

One of the most prestigious credentials in the industry, the GIA Graduate Gemologist® program gives you the comprehensive knowledge of diamonds and colored stones you need to succeed anywhere in the jewelry business. You'll gain both technical expertise and practical skills to evaluate gemstones by the 4Cs (color, clarity, cut, and carat weight), the International Diamond Grading System™, and the Colored Stone Grading System.

WHAT YOU'LL LEARN

POSSIBLE CAREER PATHS

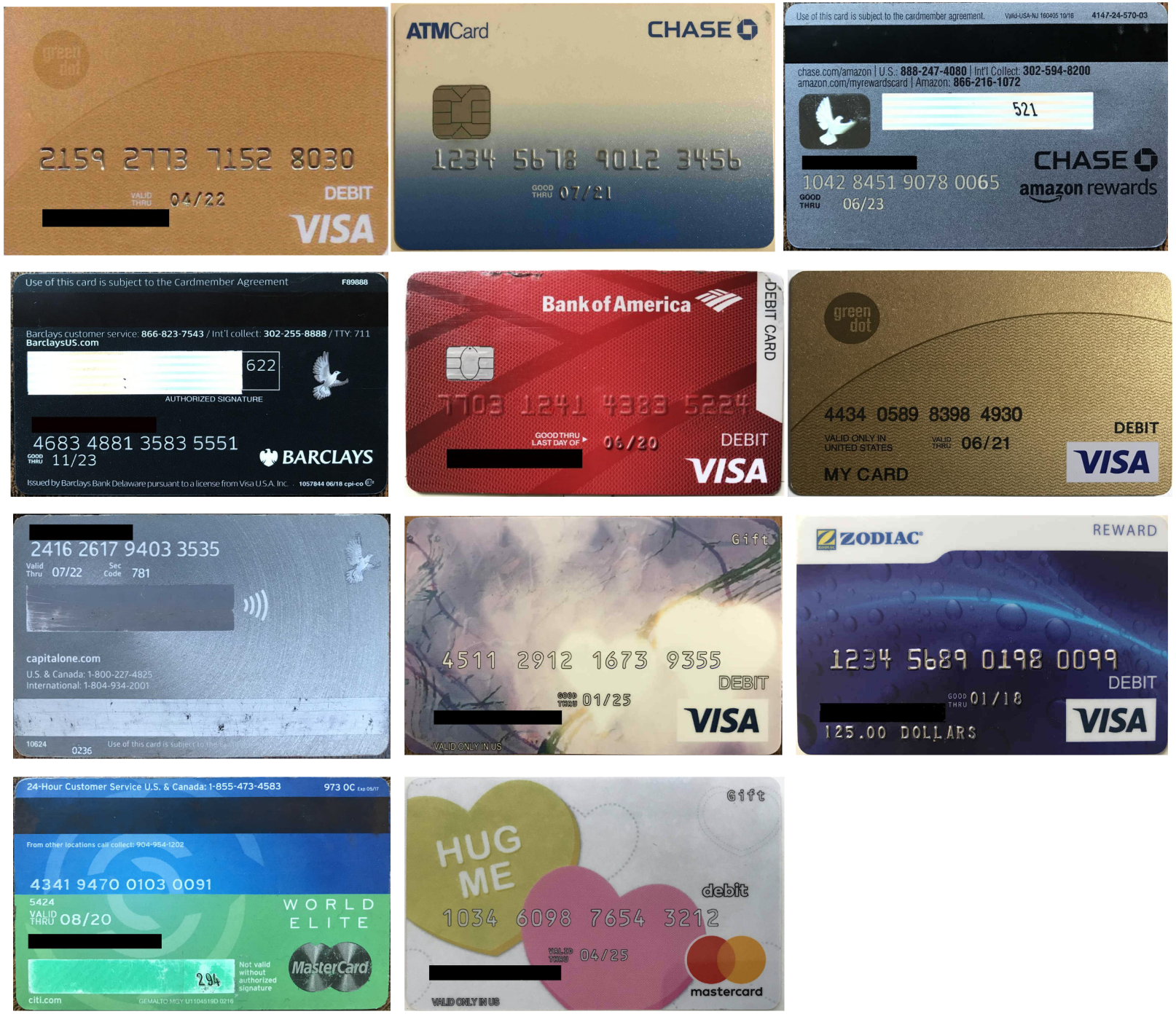
https://www.gia.edu/gem-education/program-graduate-gemologist

May be look at credit cards, instead

You’re Don the Jeweler, pick the fugazi!

You’re Don the Jeweler, pick the fugazi!

Can we detect ***high-quality*** fakes?



But why do we care?

Card not present fraud: What and How?

Card not present fraud happens when fraudsters steal credit card credentials of other people

Image from "The Security Challenges of the Rhythmprint Authentication", Wongnarukane et al.

Card not present fraud: What and How?

Card not present fraud happens when fraudsters steal credit card credentials of other people

And use these stolen credentials to make purchases online or via an app without the physical card

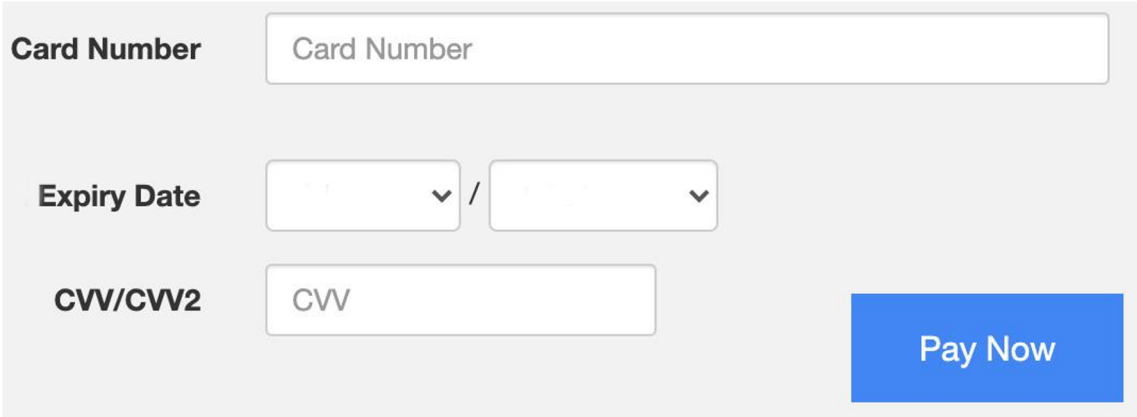


Image from "The Security Challenges of the Rhythmprint Authentication", Wongnarukane et al.

Card Present Transaction

Card Present Transaction

Card ***Not*** Present Transaction

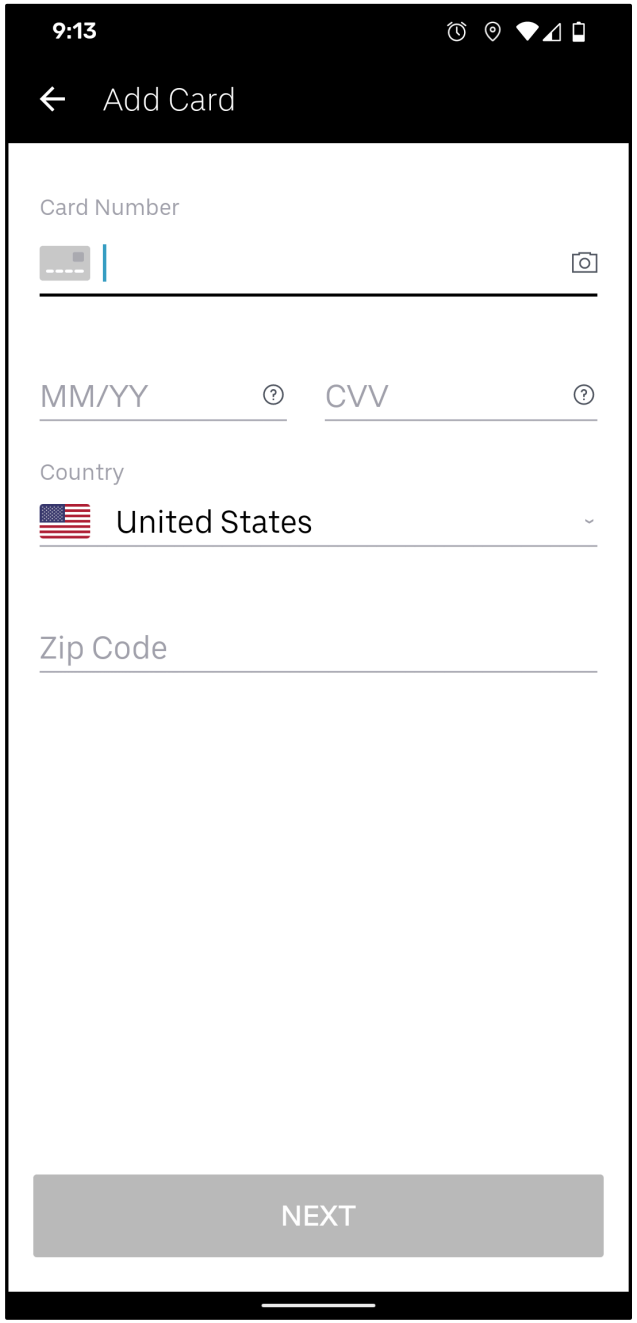
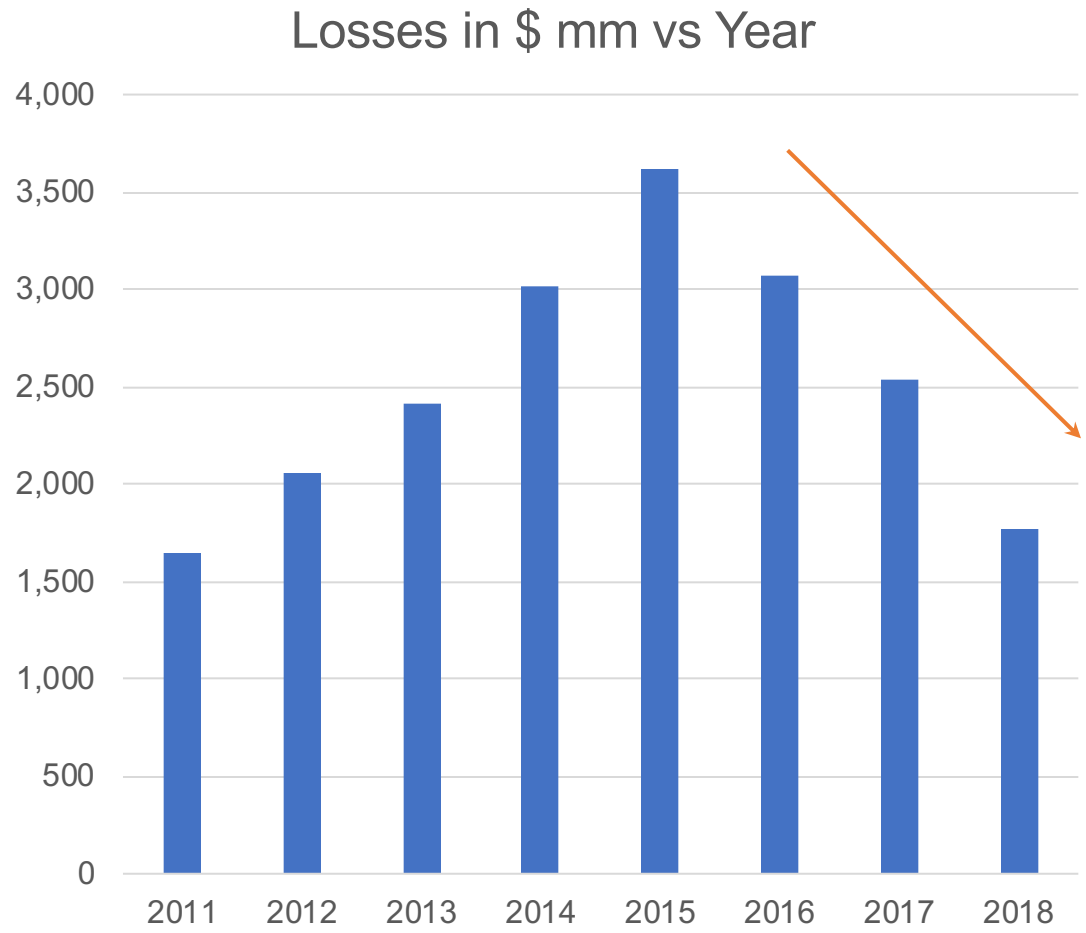


Image from UBER checkout page.

Card Present Fraud vs Card Not Present Fraud



Source: https://www.uspaymentsforum.org/wp-content/uploads/2017/03/CNP-Fraud-Around-the-World-WP-FINAL-Mar-2017.pdf
and
https://www.businesswire.com/news/home/20190102005011/en

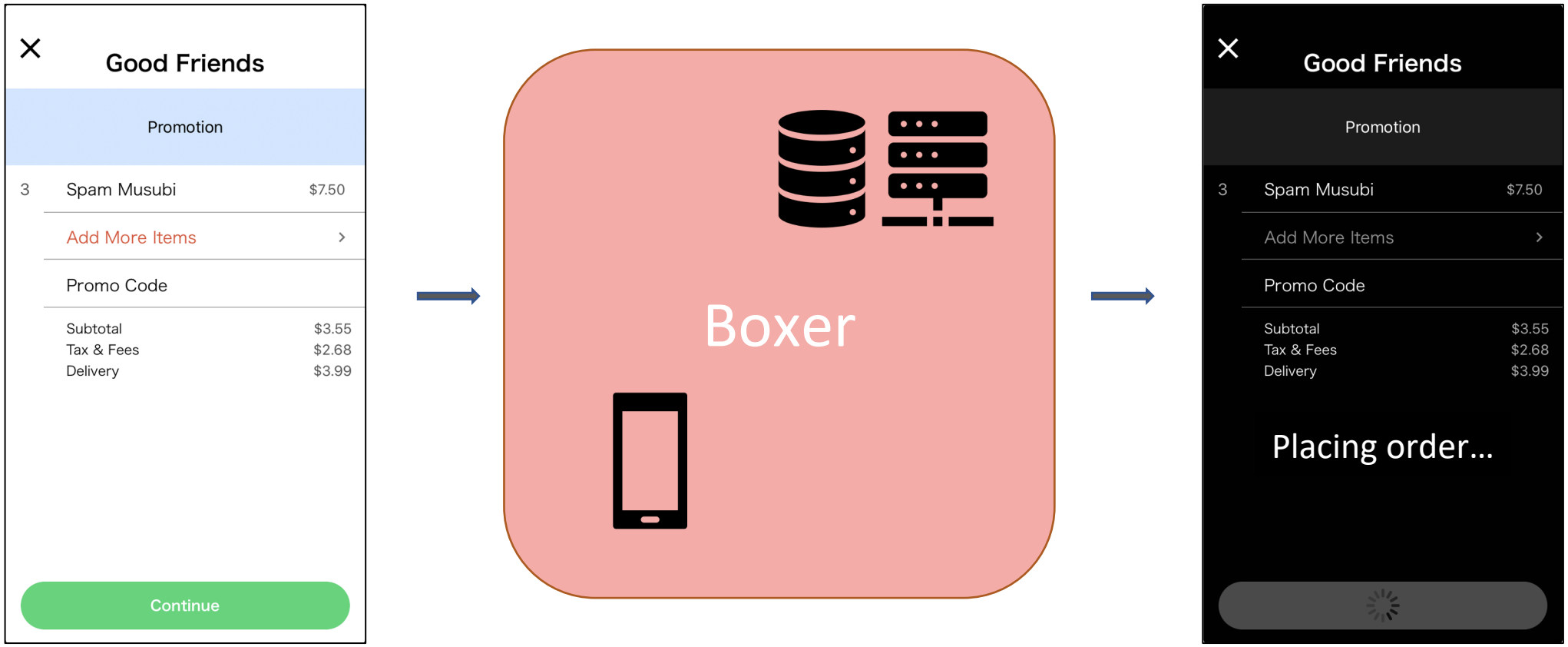
In fact, researchers found retailers will loose some ***$130 billion*** dollars in digital CNP fraud between 2018 - 2023

Source: https://www.uspaymentsforum.org/wp-content/uploads/2017/03/CNP-Fraud-Around-the-World-WP-FINAL-Mar-2017.pdf
https://www.businesswire.com/news/home/20190102005011/en
Juniper Research

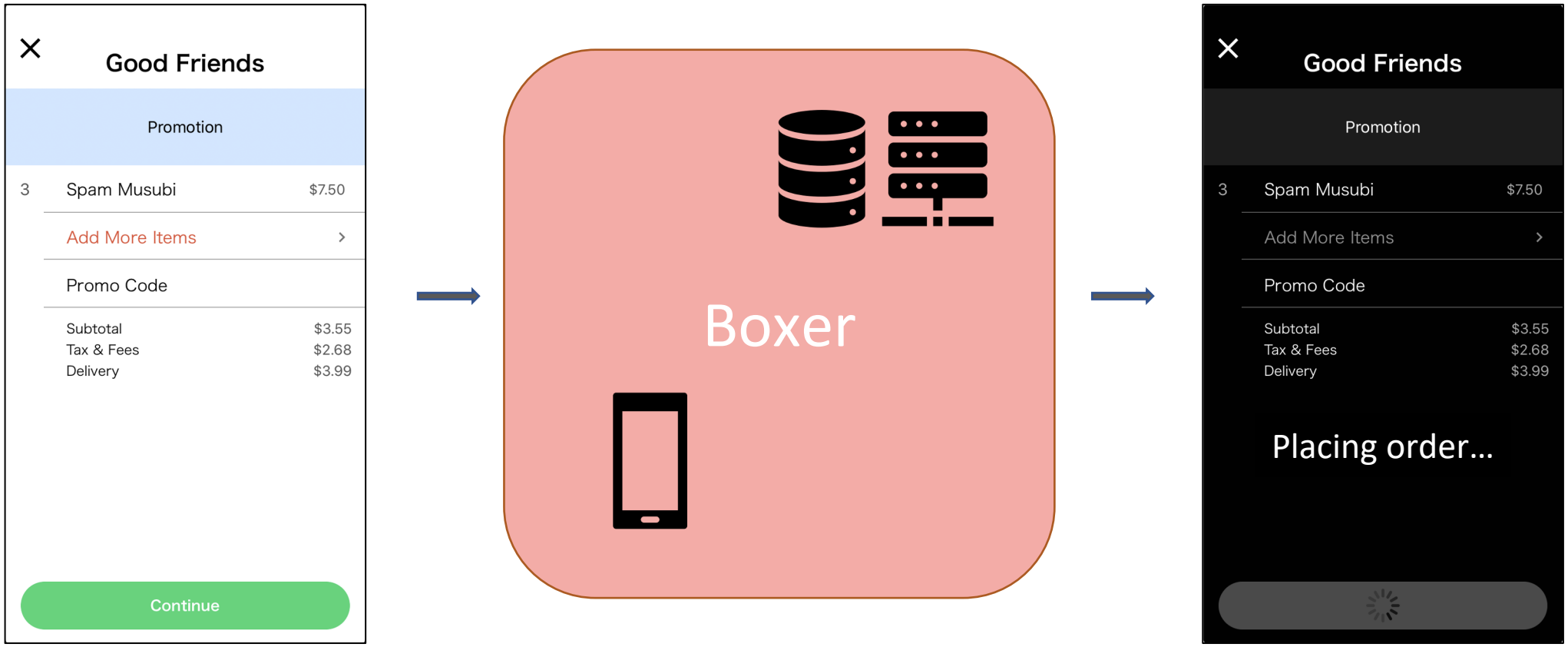
BOXER

https://www.animatedimages.org/img-animated-boxing-image-0031-88330.htm

Boxer: Client-side SDK and server to deter CNP fraud.

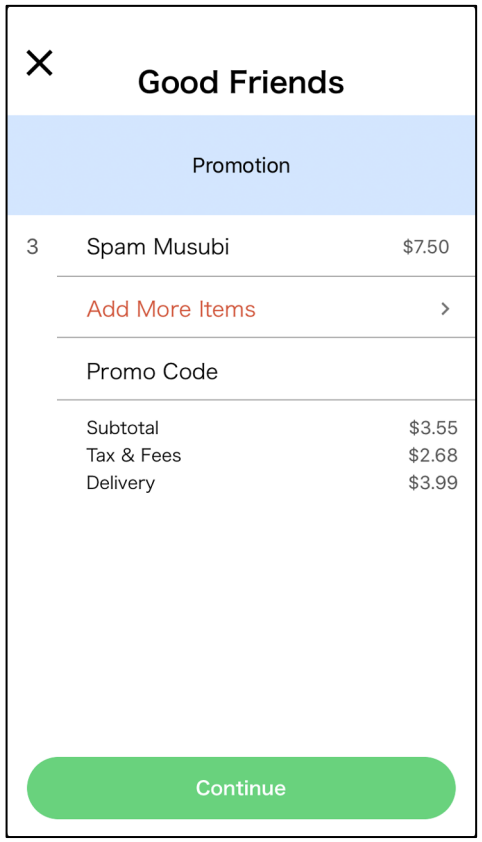


Boxer: How does it work

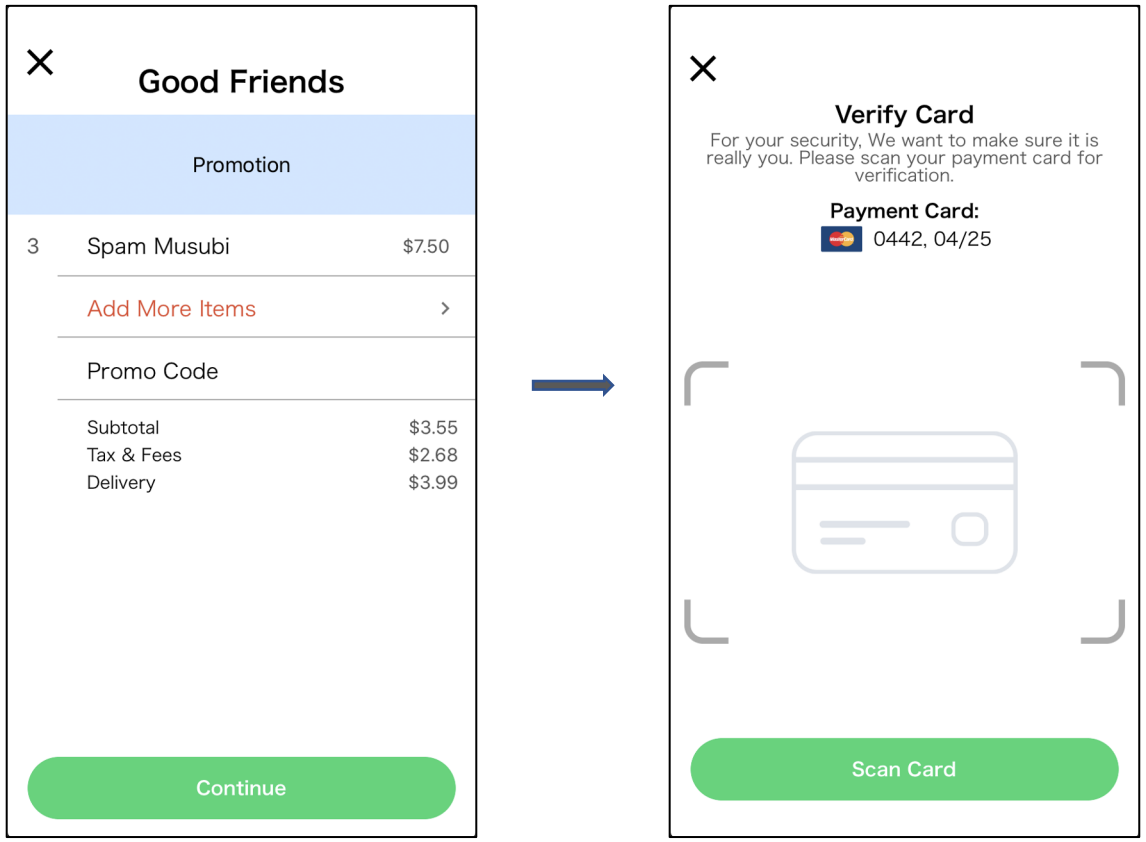


Boxer is used by the food delivery app to verify a suspicious transaction

Overview: App detects a suspicious transaction and forwards the user to Boxer.

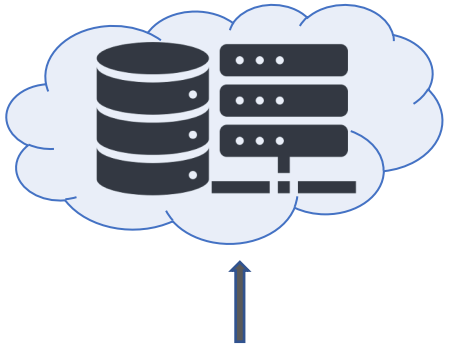


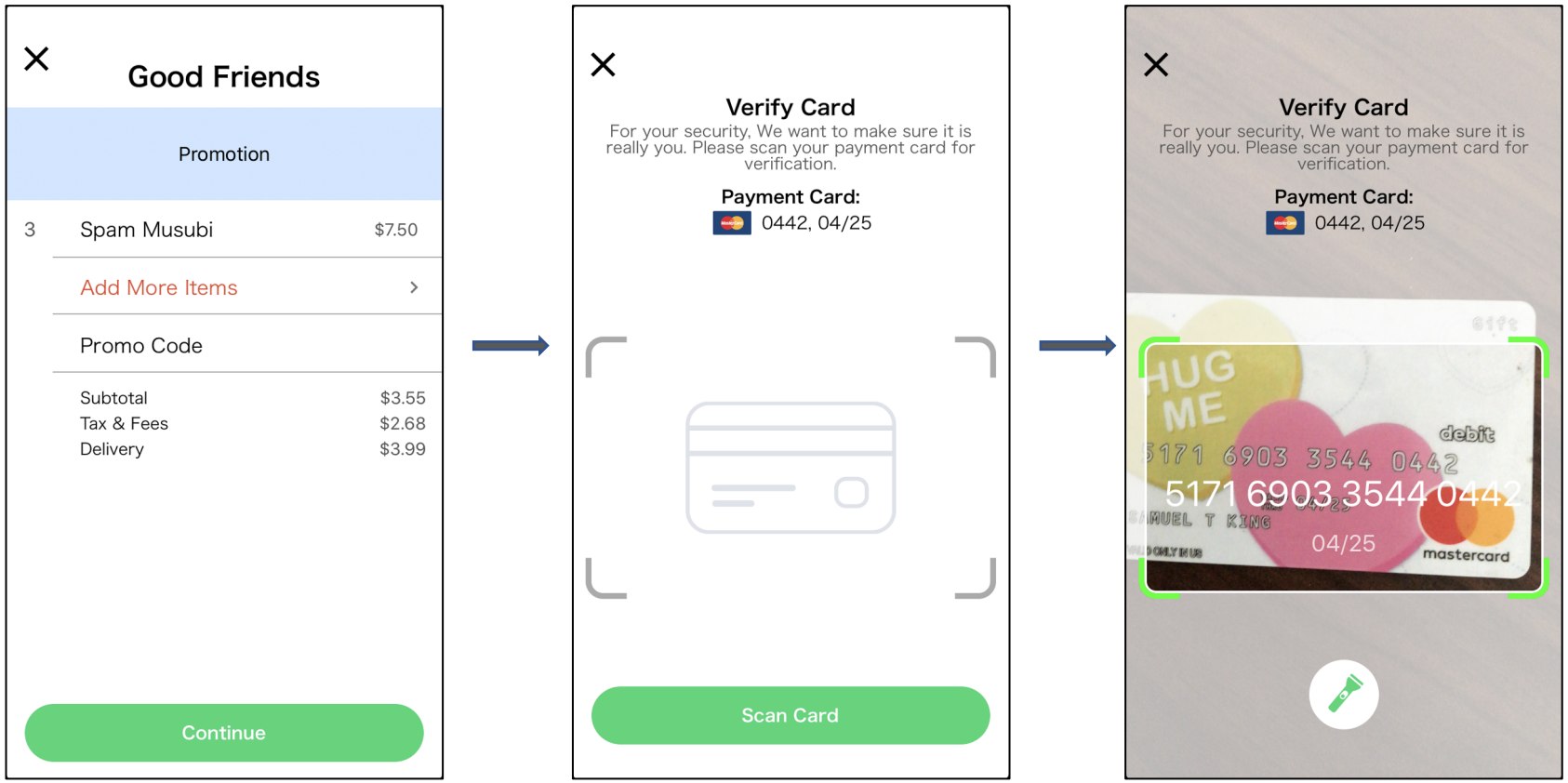
Overview: Boxer’s asks the user to scan their card.



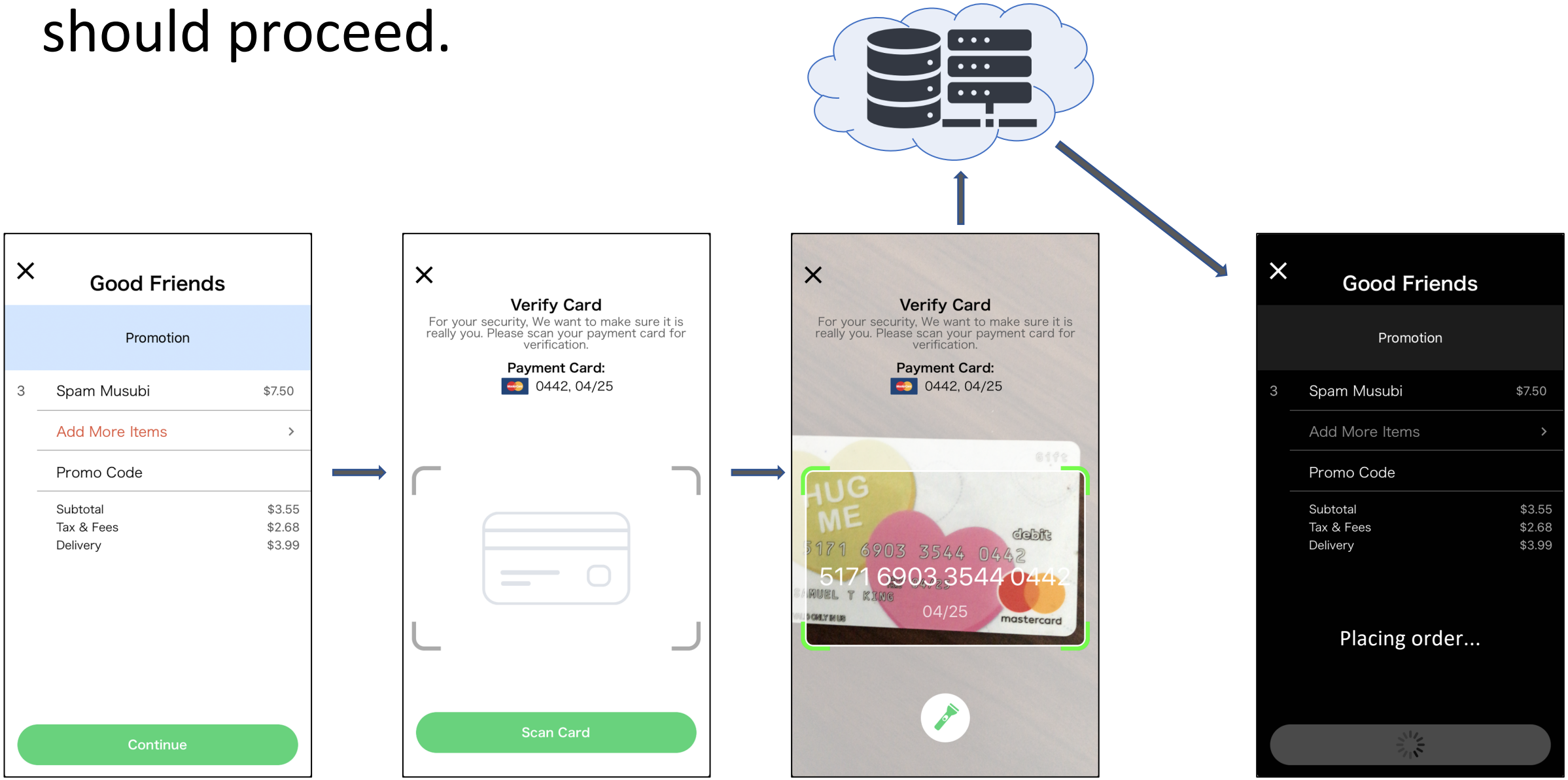
Boxer performs OCR, analyzes the video frames for telltale signs of attacks and collects device signals

Overview: Boxer's client SDK sends this data to the Boxer server.

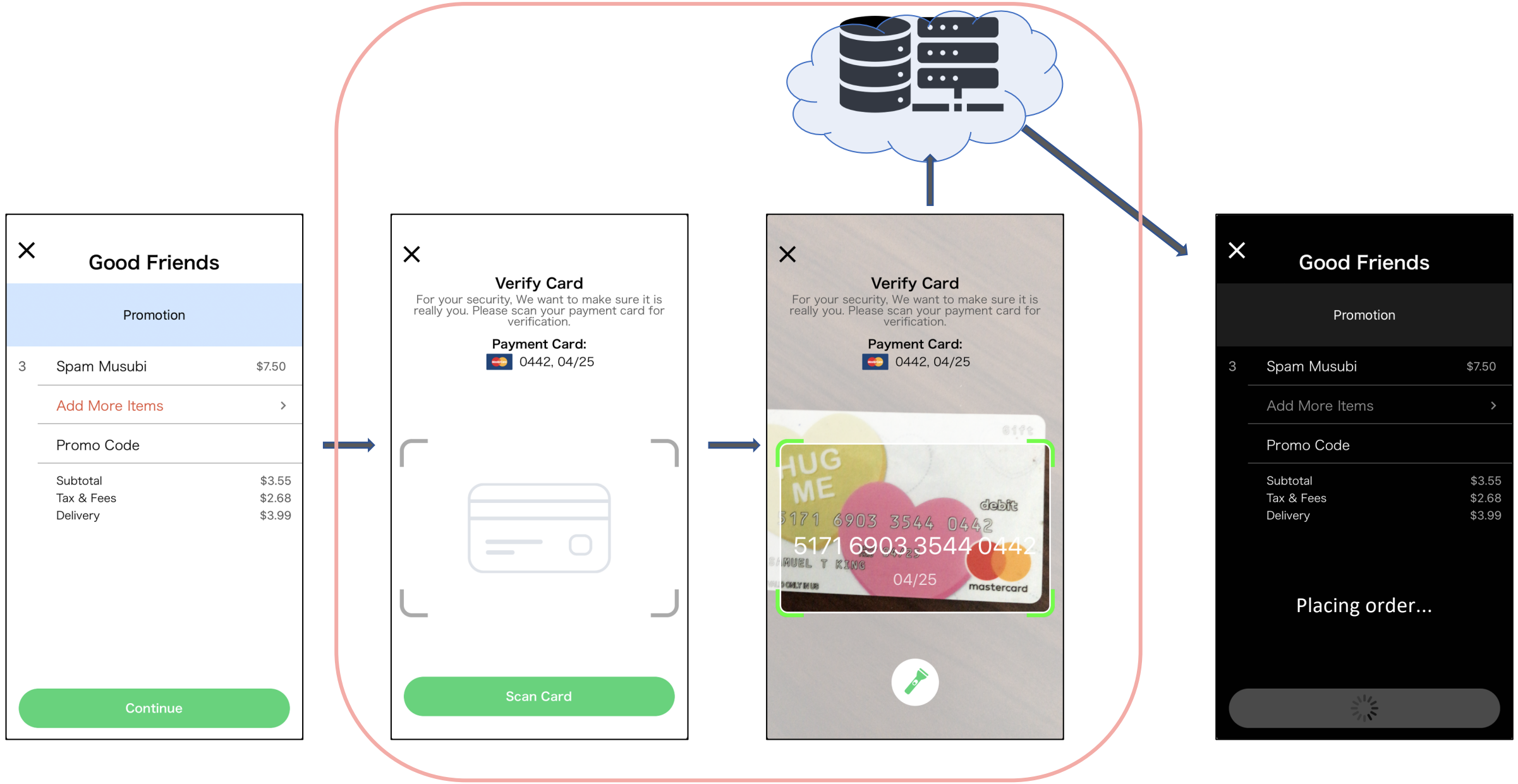




Overview: Boxer's server decides if the transaction should proceed.



Boxer: Client SDK and server



Outline

Image Analysis

Device Signals

Principles

Evaluation

Impact

Conclusions

Image Analysis: OCR

Scan the card to extract card number and expiry and check what is on record

- Perform OCR on the card number and expiry

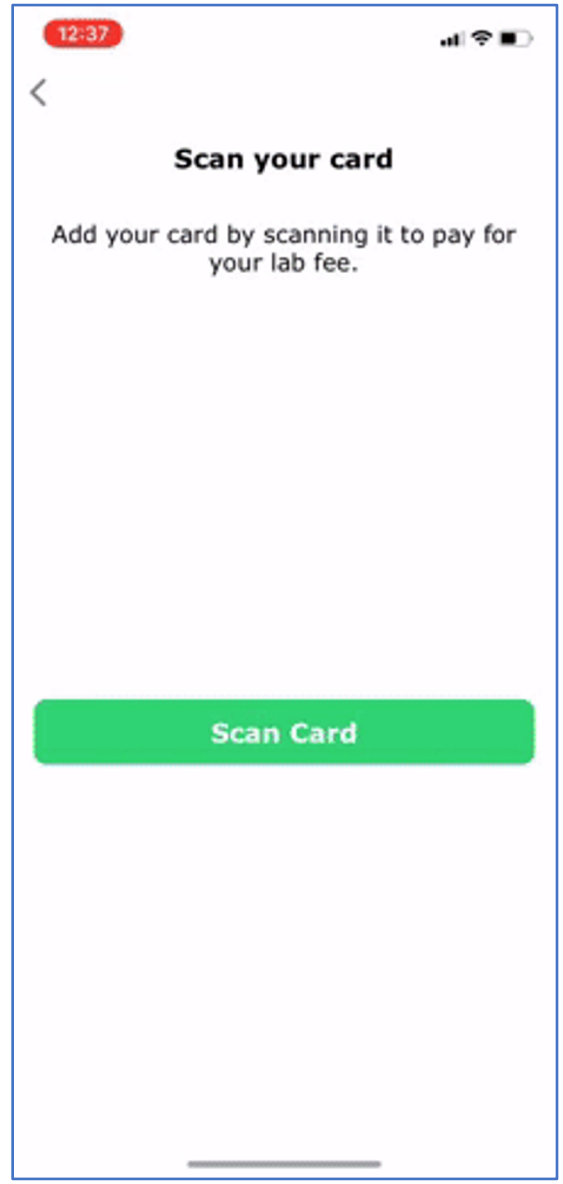


Image Analysis: BIN Check

Inspect the card image for tell tale signs of tampering.

- The image on the top has a Green Dot card number but no objects (like payment network, logo, etc.,)

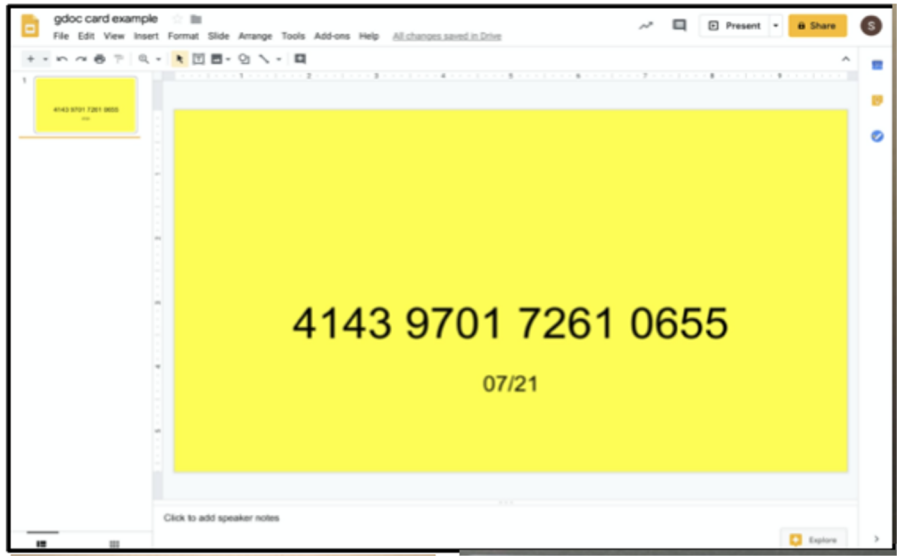


Image Analysis: BIN Check

Inspect the card image for tell tale signs of tampering.

- The image on the top has a Green Dot card number but no objects (like payment network, logo, etc.,)
- The image on the bottom has a Green Dot BIN but a CHASE logo.

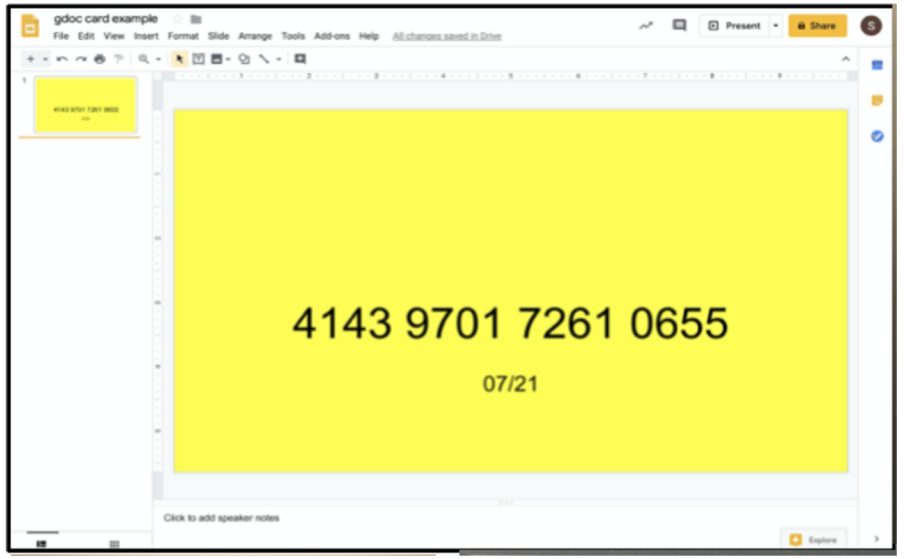


Image Analysis: Screen Detection

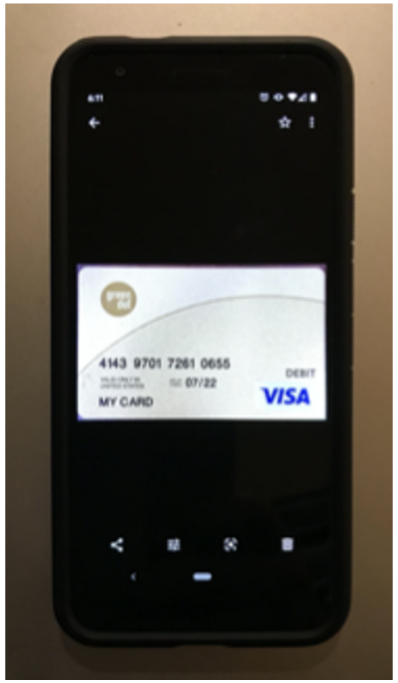
Detect ways of rendering fake card images.

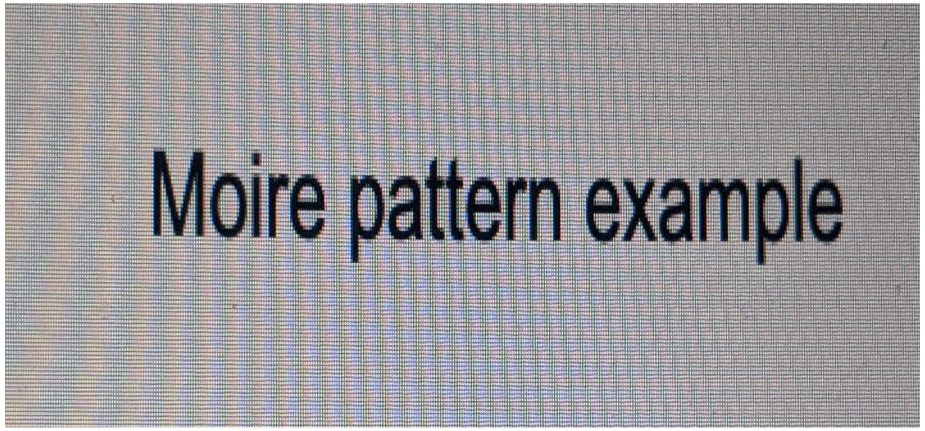
- Detect a card image scanned off a phone by homing in on the edges

Image Analysis: Screen Detection

Detect ways of rendering fake card images.

- Detect a card image scanned off a phone by homing in on the edges
- Detect computer screens by detecting Moiré patterns

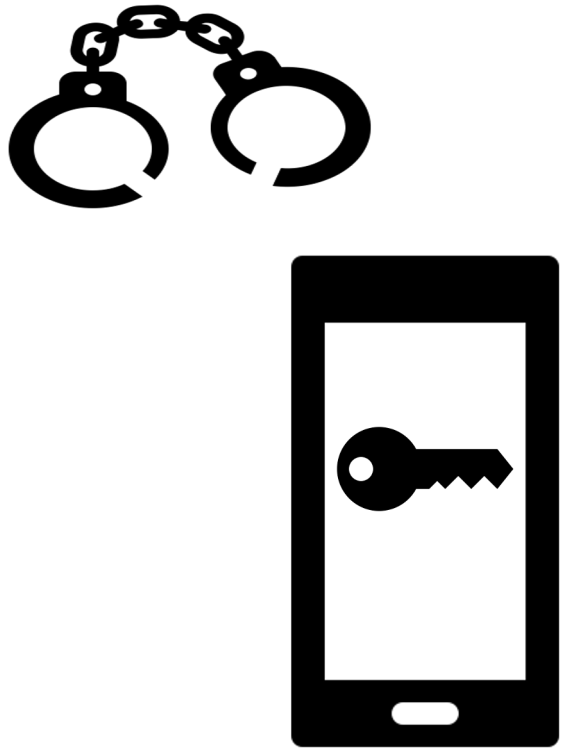




Device Signals: DeviceCheck and SafetyNet

Force the attacker to use genuine hardware and the real app.

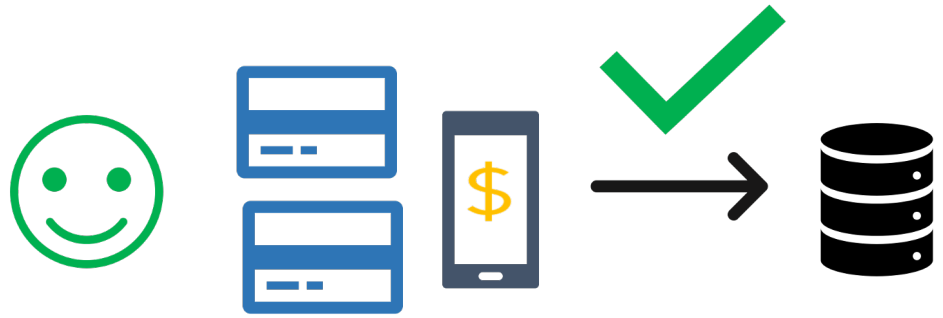
- Use the private key embedded in the hardware to verify it is genuine



Device Signals: Secure Counting

Associate attacker activities with things that are expensive like iPhones and use that to rate limit.

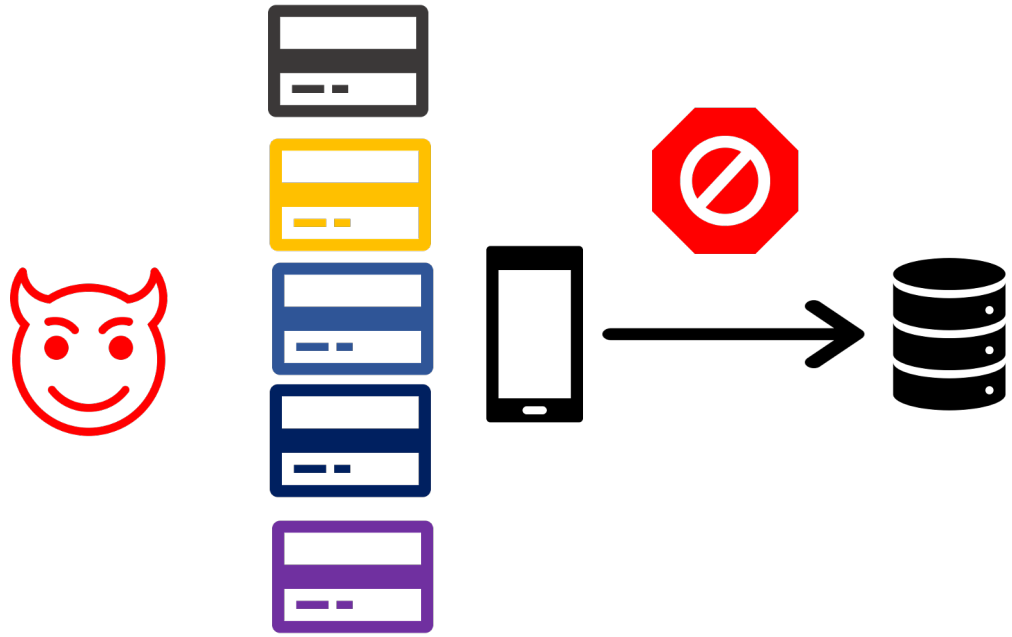
- Track activities and increment a secure counter when these occur on the same device.



Device Signals : Secure Counting

Associate attacker activities with things that are expensive like iPhones and use that to rate limit.

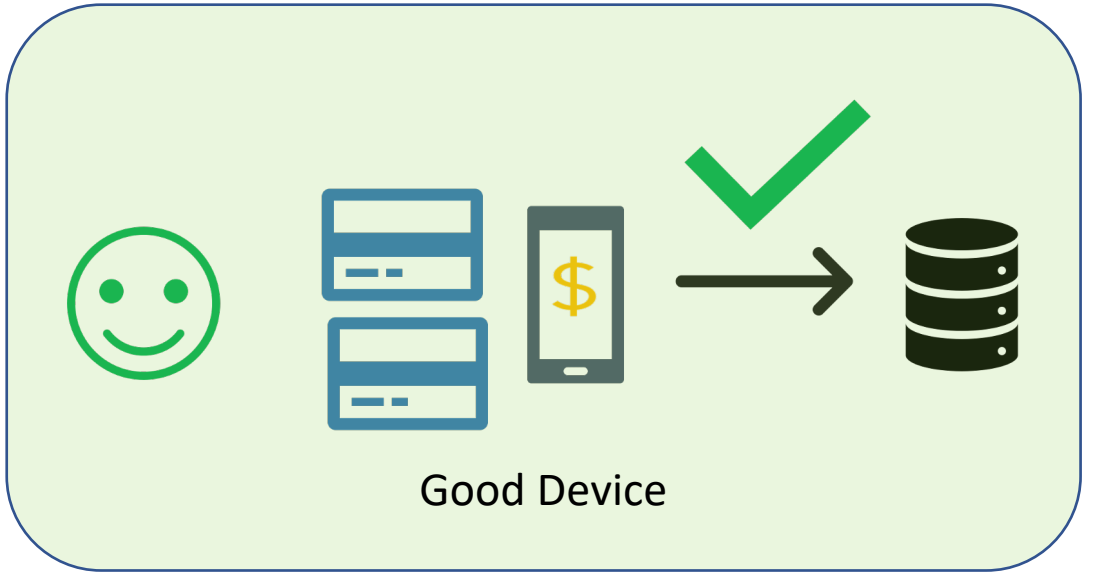
- Track activities and increment a secure counter when these occur on the same device.
- For instance, counting the number of cards added per device can limit the damage done by large scale hardware-based attacks.

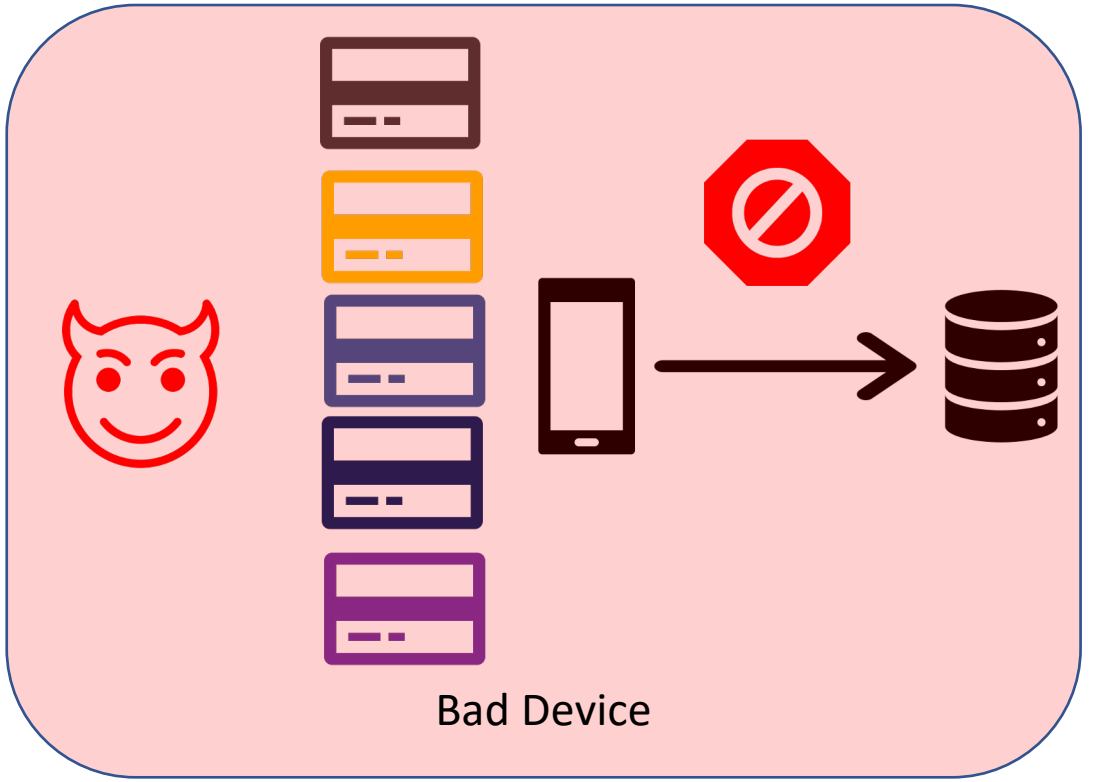


Device Signals : Secure Counting

Associate attacker activities with things that are expensive like iPhones and use that to rate limit.

- Track activities and increment a secure counter when these occur on the same device.
- For instance, counting the number of cards added per device can limit the damage done by large scale hardware-based attacks.
- Boxer’s secure counter is privacy preserving since it only identifies classes of devices and not each individual device.





Boxer design principles

Scan

Scan the card to extract relevant details and check what is on record

Inspect

Inspect the card image for tell tale signs of tampering.

Detect

Detect ways of rendering fake card images.

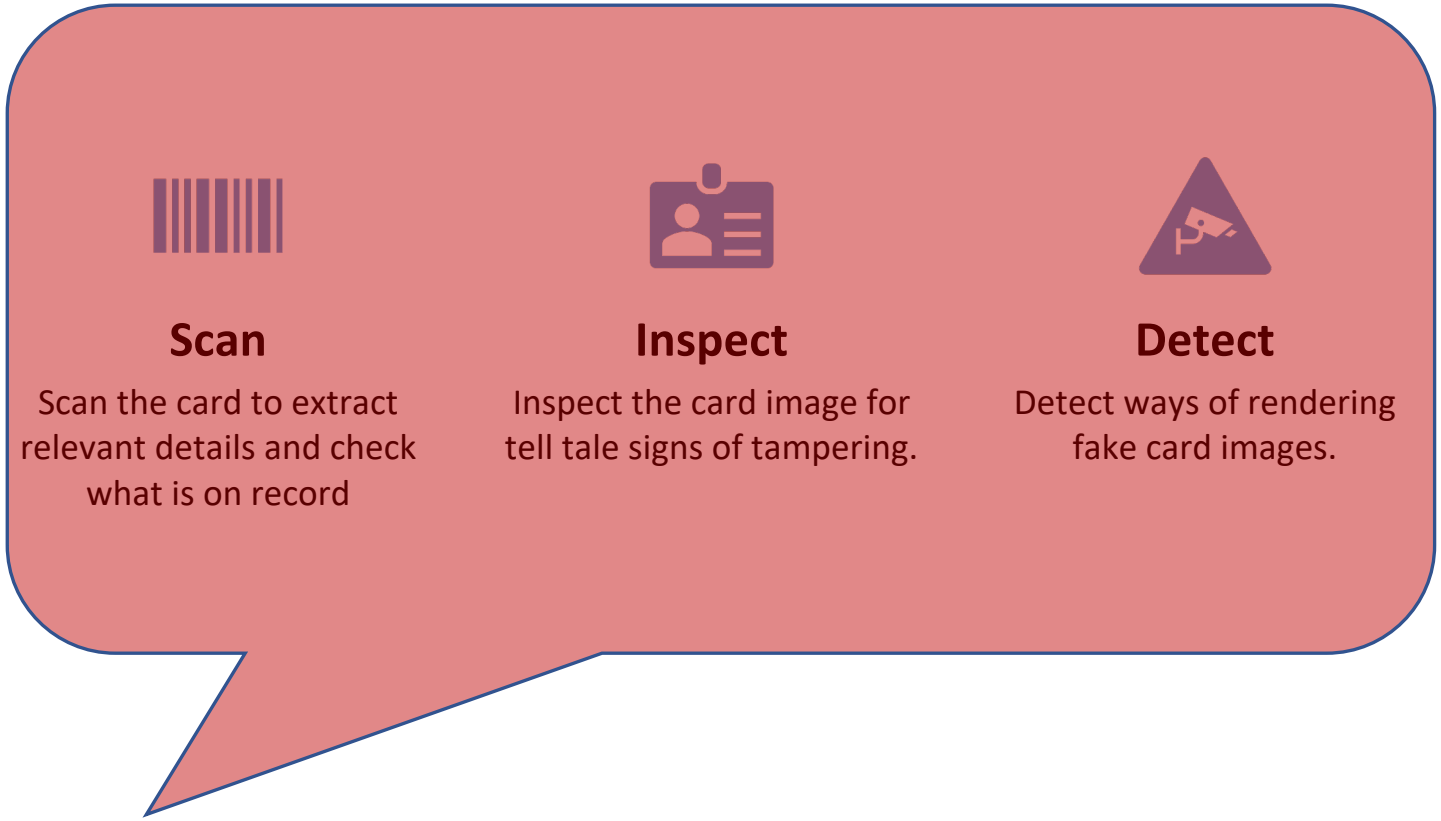
Force

Force the attacker to use genuine hardware

Associate

Associate attacker activities with things that are expensive for secure rate limiting.

Boxer design principles



Scan

Scan the card to extract relevant details and check what is on record

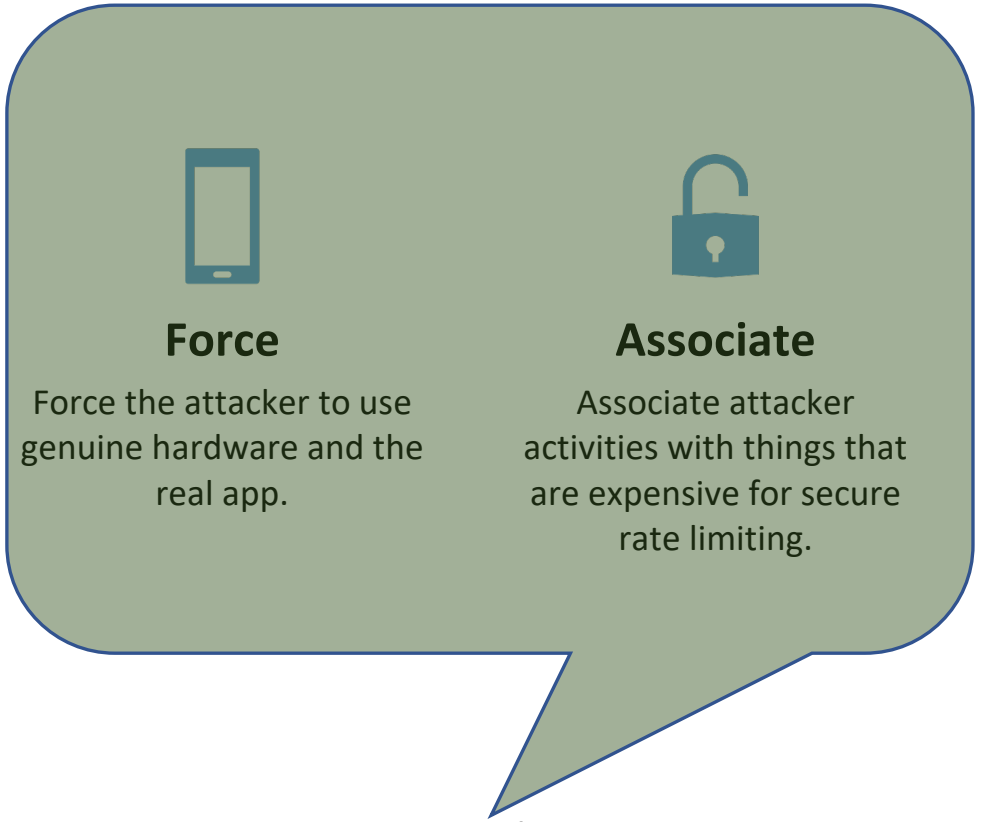
Inspect

Inspect the card image for tell tale signs of tampering.

Detect

Detect ways of rendering fake card images.

Image analysis



Force

Force the attacker to use genuine hardware and the real app.

Associate

Associate attacker activities with things that are expensive for secure rate limiting.

Device signals

Boxer design principles

Scan

Scan the card to extract relevant details and check what is on record

Inspect

Inspect the card image for tell tale signs of tampering.

Detect

Detect ways of rendering fake card images.

Force

Force the attacker to use genuine hardware

Associate

Associate attacker activities with things that are expensive for secure rate limiting.

Boxer design principles

Scan

Scan the card to extract relevant details and check what is on record

Inspect

Inspect the card image for tell tale signs of tampering.

Detect

Detect ways of rendering fake card images.

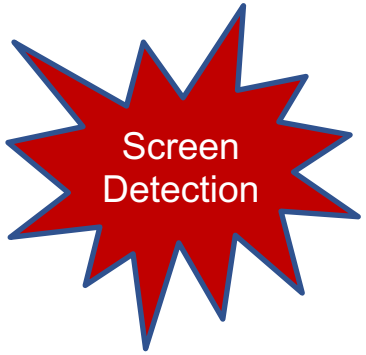
Force

Force the attacker to use genuine hardware

Associate

Associate attacker activities with things that are expensive for secure rate limiting.

Boxer design principles



Scan

Scan the card to extract relevant details and check what is on record

Inspect

Inspect the card image for tell tale signs of tampering.

Detect

Detect ways of rendering fake card images.

Force

Force the attacker to use genuine hardware

Associate

Associate attacker activities with things that are expensive for secure rate limiting.

Boxer design principles

Scan

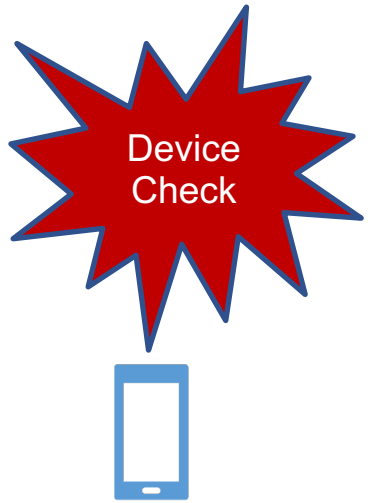
Scan the card to extract relevant details and check what is on record

Inspect

Inspect the card image for tell tale signs of tampering.

Detect

Detect ways of rendering fake card images.



Force

Force the attacker to use genuine hardware

Associate

Associate attacker activities with things that are expensive for secure rate limiting.

Boxer design principles

Scan

Scan the card to extract relevant details and check what is on record

Inspect

Inspect the card image for tell tale signs of tampering.

Detect

Detect ways of rendering fake card images.

Force

Force the attacker to use genuine hardware

Associate

Associate attacker activities with things that are expensive for secure rate limiting.

Evaluation: Boxer's net effect end to end.

We report results from an app that allowed users flagged by their system to verify themselves with Boxer.

For two weeks in February 2020, **45** users were sent to Boxer for verification.

Evaluation: Boxer’s net effect end to end.

35 of these users failed OCR and were blocked by Boxer.

A manual review by the app later confirmed all **35** users to have been fraudulent.

Evaluation: Boxer's net effect end to end.

Of the remaining users, **8** passed Boxer's challenge and were allowed to complete their transactions.

A manual review conducted by the app later confirmed Boxer's decisions to be accurate.

Evaluation: Boxer's net effect end to end.

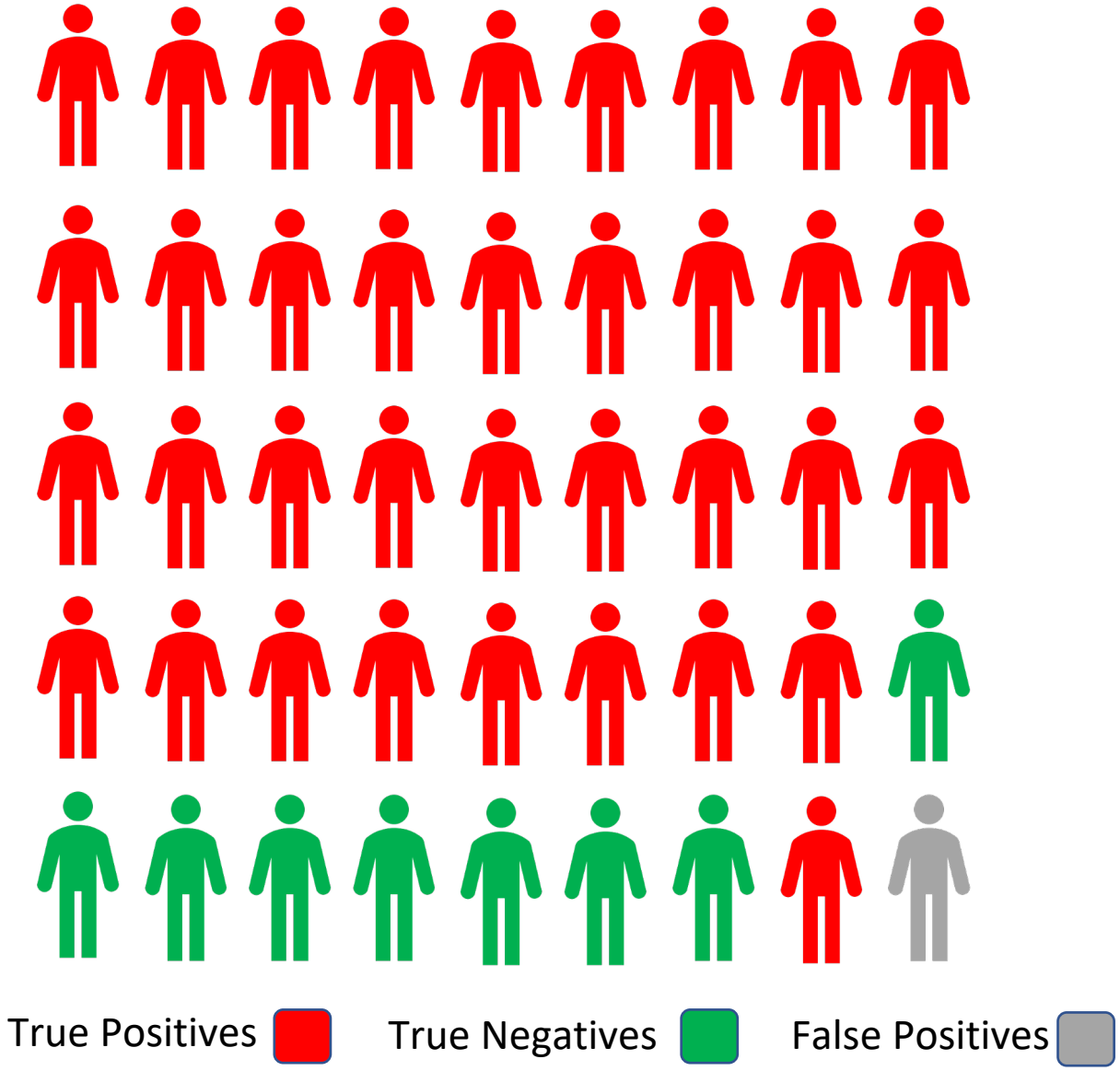
Of the remaining **2** users, one was caught by Boxer's secure counter and the other was flagged by Boxer's screen detection.

The user caught by secure counter was confirmed by manual review to be a fraudster.

The other user caught by screen detection was confirmed to be a false positive by manual review.

Evaluation: Boxer's net effect end to end.

Thus, Boxer recovered **89%** of the app's legitimate users without incurring additional fraud.



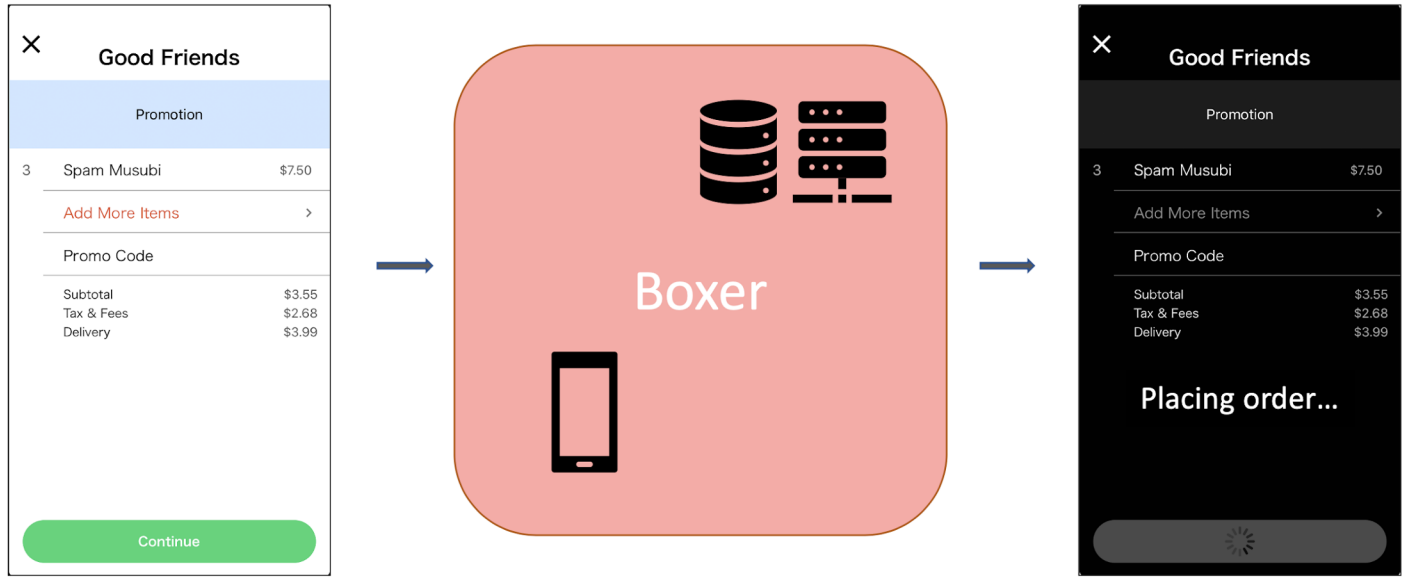
Impact

So far 323 apps have integrated Boxer, many of them have deployed Boxer in production.

Boxer has scanned over 10 million cards and is currently actively stopping fraud.

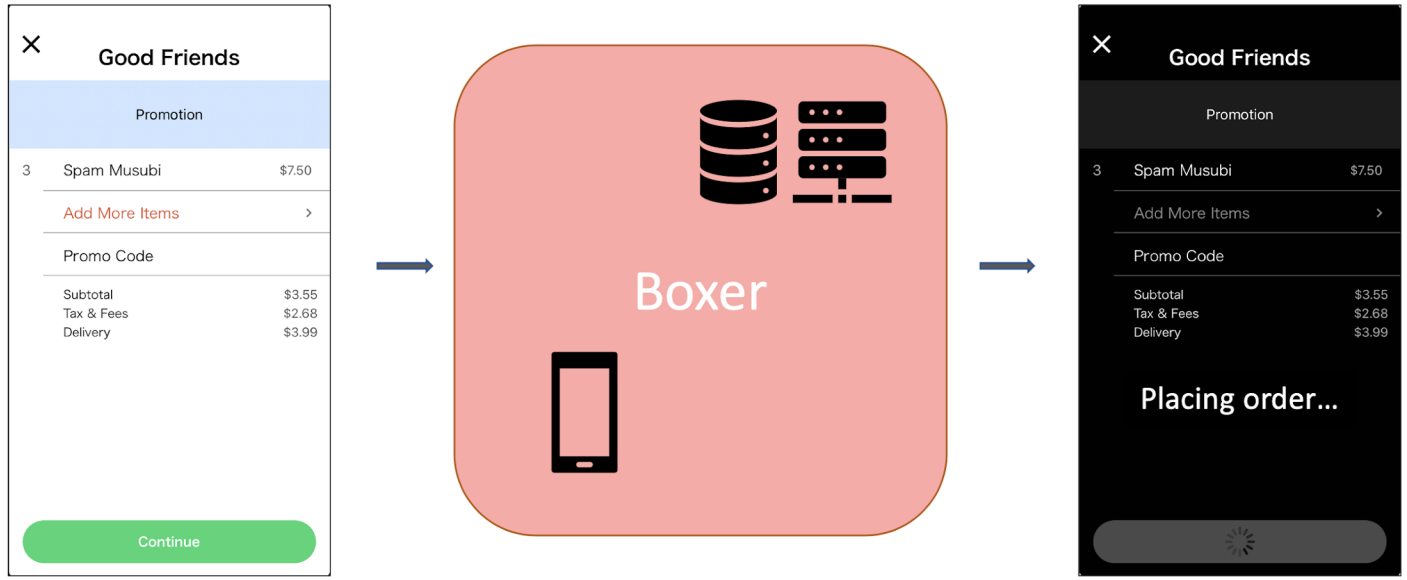
Conclusions

We introduced Boxer, a client-side SDK and server for preventing card-not-present-fraud.

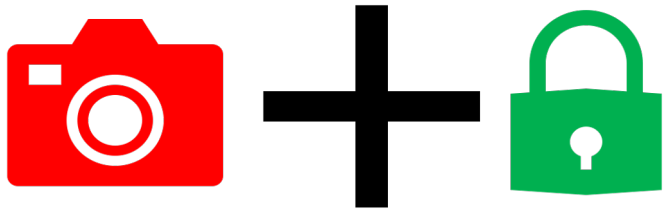


Conclusions

We introduced Boxer, a client-side SDK and server for preventing card-not-present-fraud.



Boxer combines multiple image analysis techniques with a novel secure counting abstraction to provide a holistic solution to CNP attacks.

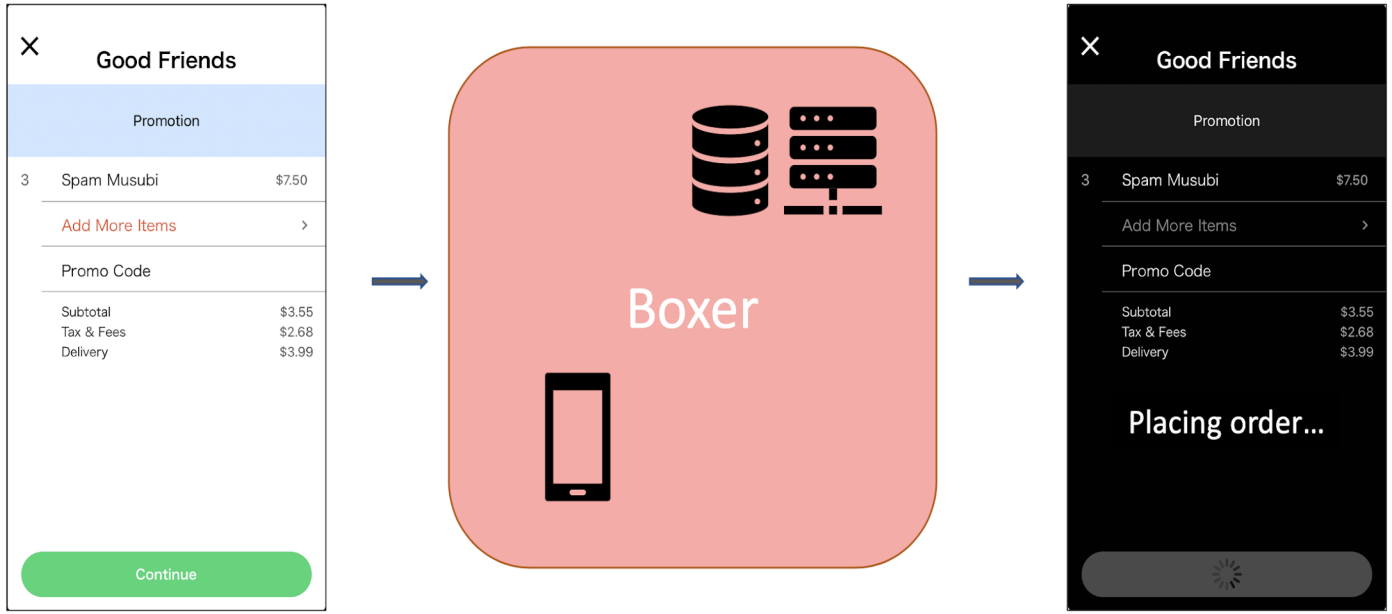


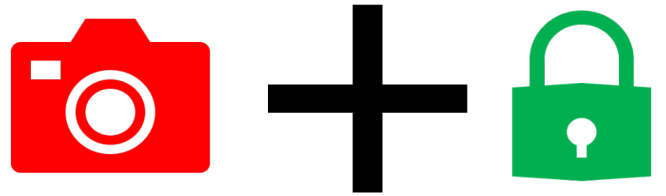
Conclusions

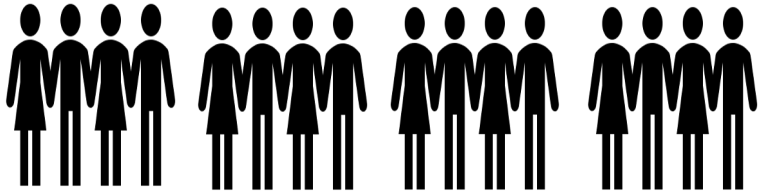
We introduced Boxer, a client-side SDK and server for preventing card-not-present-fraud.

Boxer combines multiple image analysis techniques with a novel secure counting abstraction to provide a holistic solution to CNP attacks.

Boxer has been integrated into 323 apps. It has scanned 10 millions cards already and is currently actively stopping fraud in production.







Thank you.

Please email your questions to:

zdin@ucdavis.edu

or

hvenugopalan@ucdavis.edu