Parking Australia – Cyber Security Forum

MELBOURNE
15th February 2023 | SleevesUP, Cremorne Victoria

James Tin james.tin@gmail.com

Senior Director of Security and Fraud Solutions

Agenda

0 Current Threat Landscape post Covid-19

1 Case Study – e-Commerce Customer

2 The future has no rules

3 MFA only succeeds when it fails

Standard Car vs High Performance Car

Great city car

Track = Better Tyres
Bigger Brakes
Better Suspension
Bigger Spoiler
Bigger Engine + Turbo
Better Exhaust

Who & Why?

Traditional Hackers: Glory Hounds

Political Hacktivism

But Why Do They Want to Attack Me?

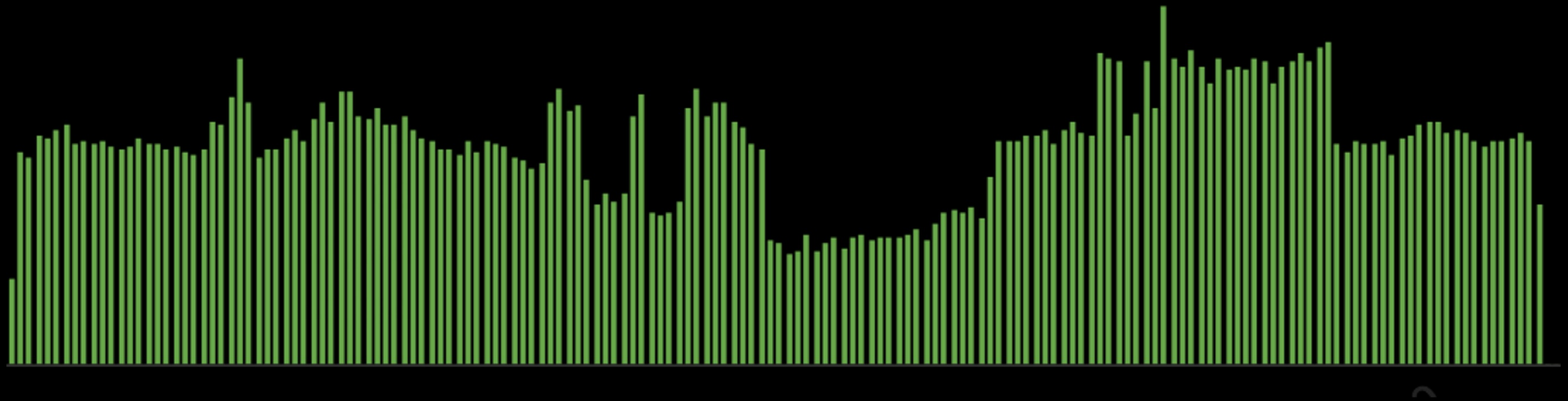
1. They want your DATA
2. They want your SERVERS
3. They want your CUSTOMERS
4. They ‘Just’ want to bring you down


Cybersecurity statistics 2017: A
swimlane.com/blog/cybersecurity-statistics-2017/
1. The volume of threat alerts has become staggering.
Alert fatigue is a very real problem for embattled SOC professionals.
With organizations receiving an average of 17,000 malware alerts per week—and of that, fewer than 20 percent worthy of examination—only 4 percent of all valid threats are actually investigated by those in the trenches.
To make matters worse, Intel Security reports that 93 percent of security personnel are overwhelmed by alert data and unable to triage all potential threats.

1

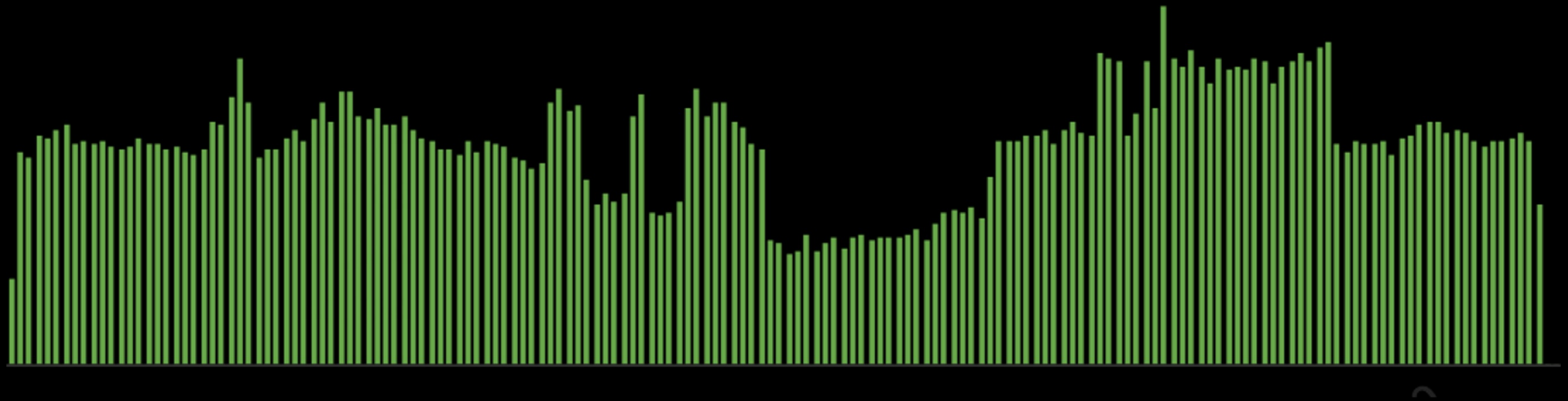
Case Study – e-Commerce Customer

Traffic at Fortune 100 customer

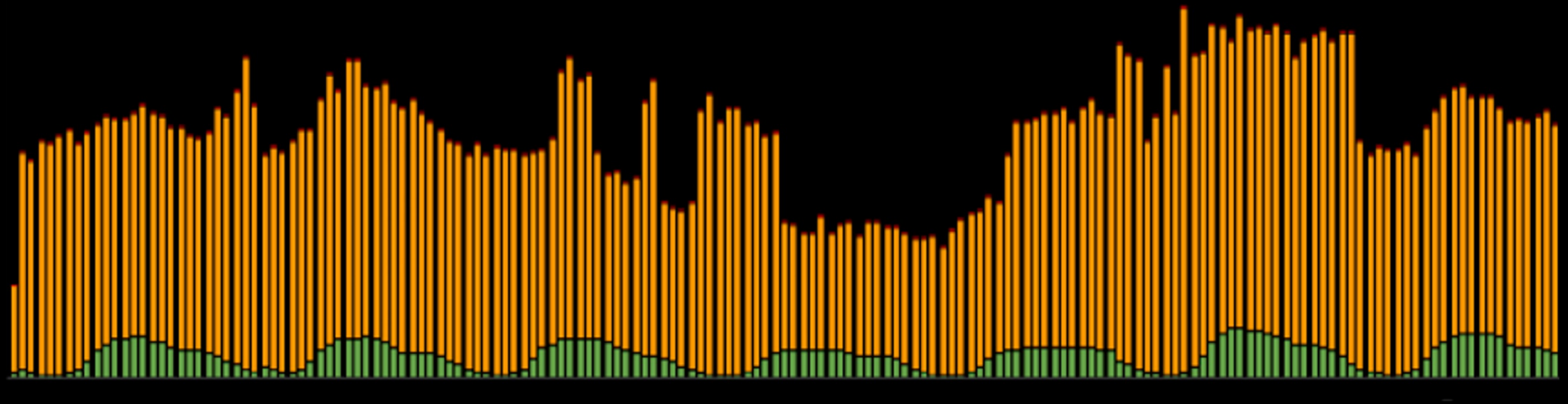


What normal traffic looks like

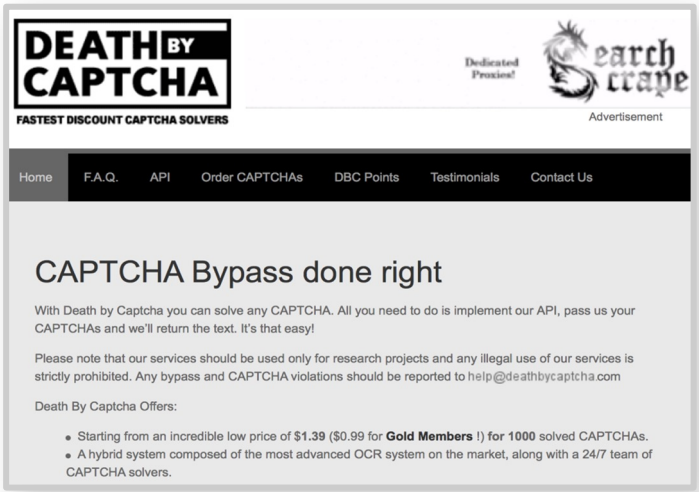
Traffic at Fortune 100 customer



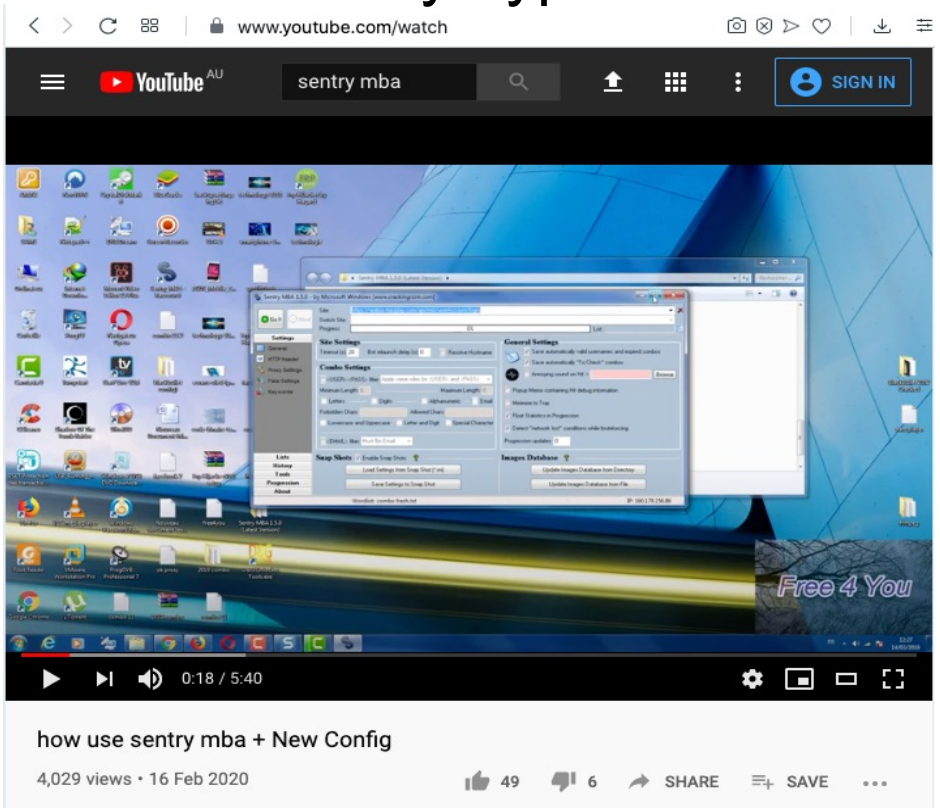
Attack traffic revealed to be >90%



Cybercriminals weaponize AI tools to easily bypass traditional security controls



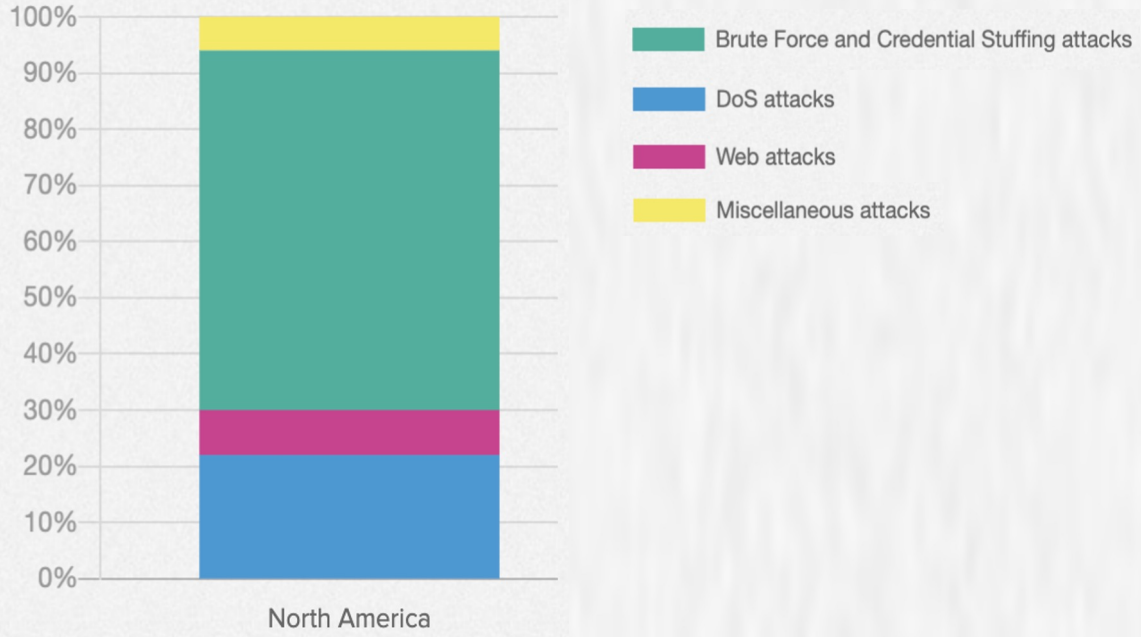
Cybercrime-as-a-Service uses AI to solve 1000 CAPTCHAs for $1.39



Google study: human solve rate for CAPTCHA: 33%

ML OCR solve rate: 99.8%

Credential stuffing exceeds DDoS attacks, globally, and is the top attack vector for financial services in the region



Source: F5 Security Incident Response Team (F5 SIRT), April 27, 2020
https://www.f5.com/labs/articles/threat-intelligence/top-attacks-against-financial-services-organizations-2017-2019

Case Study: Credential stuffing on FSI customer

Over 3 weeks our team:

- ✓ Mobile Banking mitigation attack mode monitoring and alerting to auto trigger when threshold is reached
- ✓ Mobile banking One Time Pin (OTP) invalid attempt lockout established
- ✓ Deployed ReCaptcha for Mobile Banking WAP (Web Application)
- ✓ IP Reputation and GeoIP Blocking enable on the NetScalers
- ✓ IP Reputation, GeoIP blocking and Rate Limiting on the McAfee IPS and moved to the perimeter to be inline with the firewalls in [redacted]
- ✓ ISP DDoS protection in [redacted] (rolled back due to connectivity issues with [redacted])
- ✓ Reviewed WAF options with multiple vendors
- ✓ Discuss lessons learns with other CUs
- ✓ Created Power BI reports for invalid logins to assist with forensics
- ✓ Ektron update to re-mediate vulnerability
- ✓ Communicated with key business stakeholders daily
- ✓ Meetings with client references on security tools we are considering

Once blocked, attackers resort to manual fraud

"Fullz"

Tell Us About Yourself

(All fields are required unless specified optional)

Personal Information

First Name | Middle Initial *(opt.)* | Last Name

Date of Birth

Month | Day | Year

Social Security Number

Are you a U.S. citizen?

- Yes
- No

Address and Contact Information

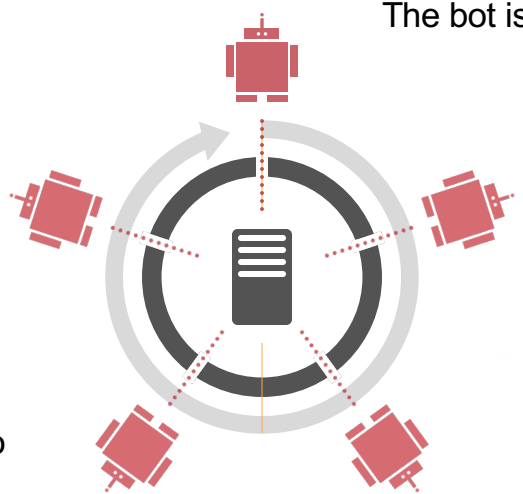
Home Address | Apt./Ste. *(opt.)* | ZIP Code

City | State

I'd like to provide a P.O. Box address. *(opt.)*

Traditional solutions

BLOCKING DOES NOT WORK



Motivation
The bot is here to get something

Blocking
Prevents the bot from getting what it came for

Evasion
Operator modifies the bot to evade detection / mitigation

Awareness
Blocking also alerts bot operator

2

The future has no Rules

Instead of *rigid rules*, we need *durable descriptions* of how fraud flows across the seams

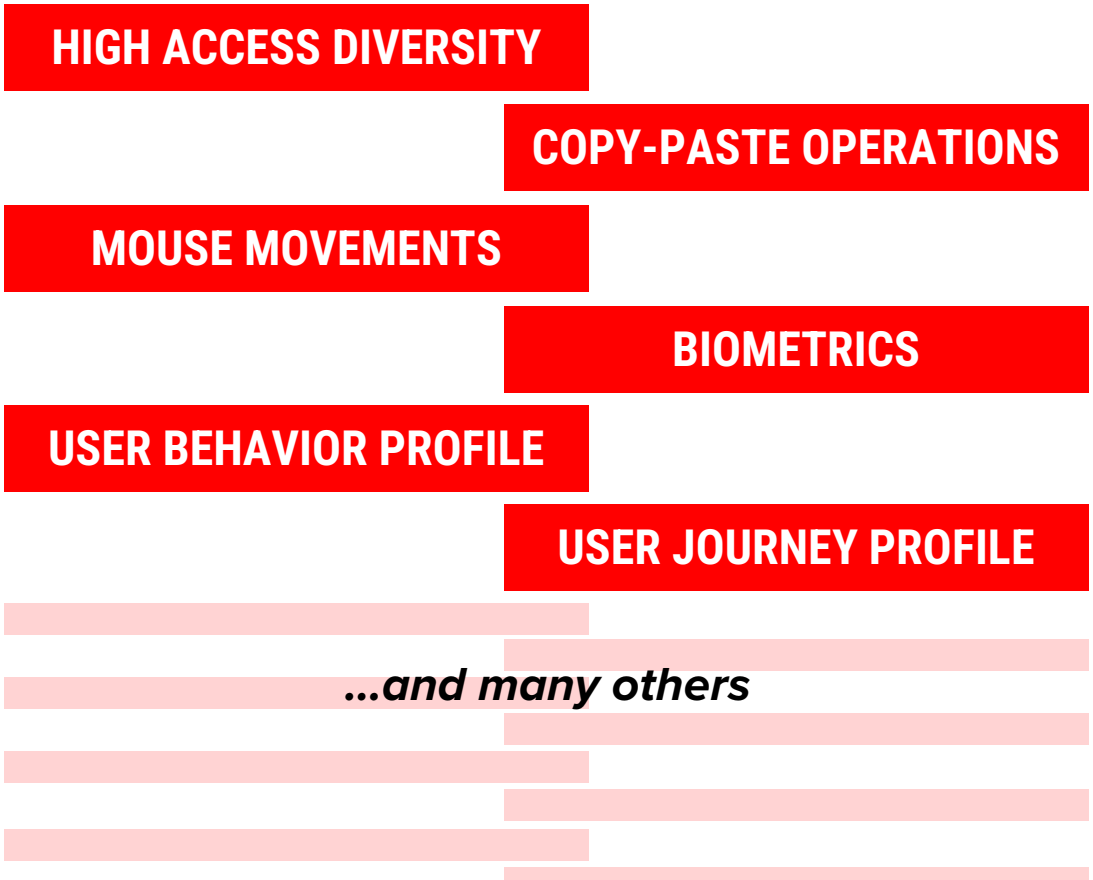
Across network security, application security, fraud and identity, B2C enterprises today needs to answer 3 fundamental questions:

Are you human?

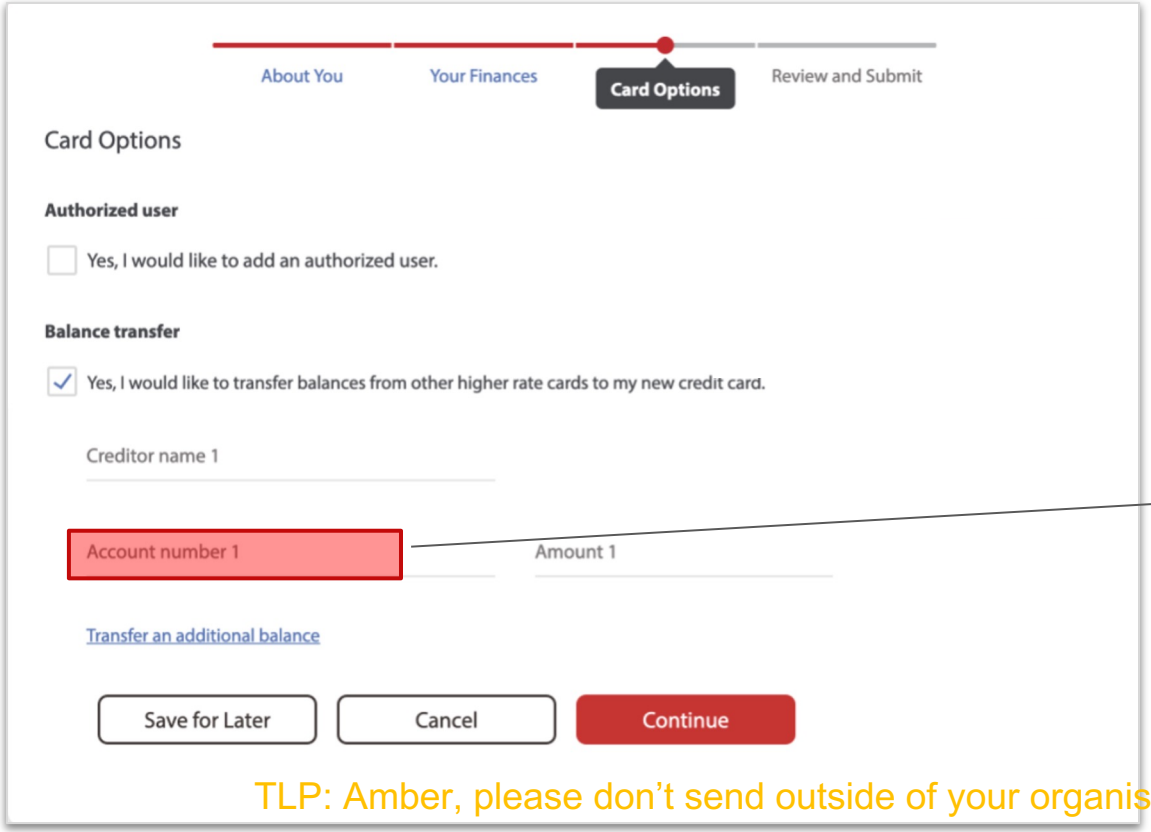
Are you good or bad?

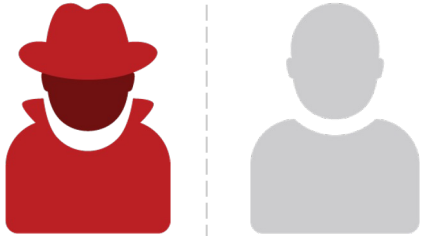
Are you who you say you are?

Human-comprehensible indicators used in fraud systems



Fraudsters are 250x more likely to use Ctrl-V than legitimate users



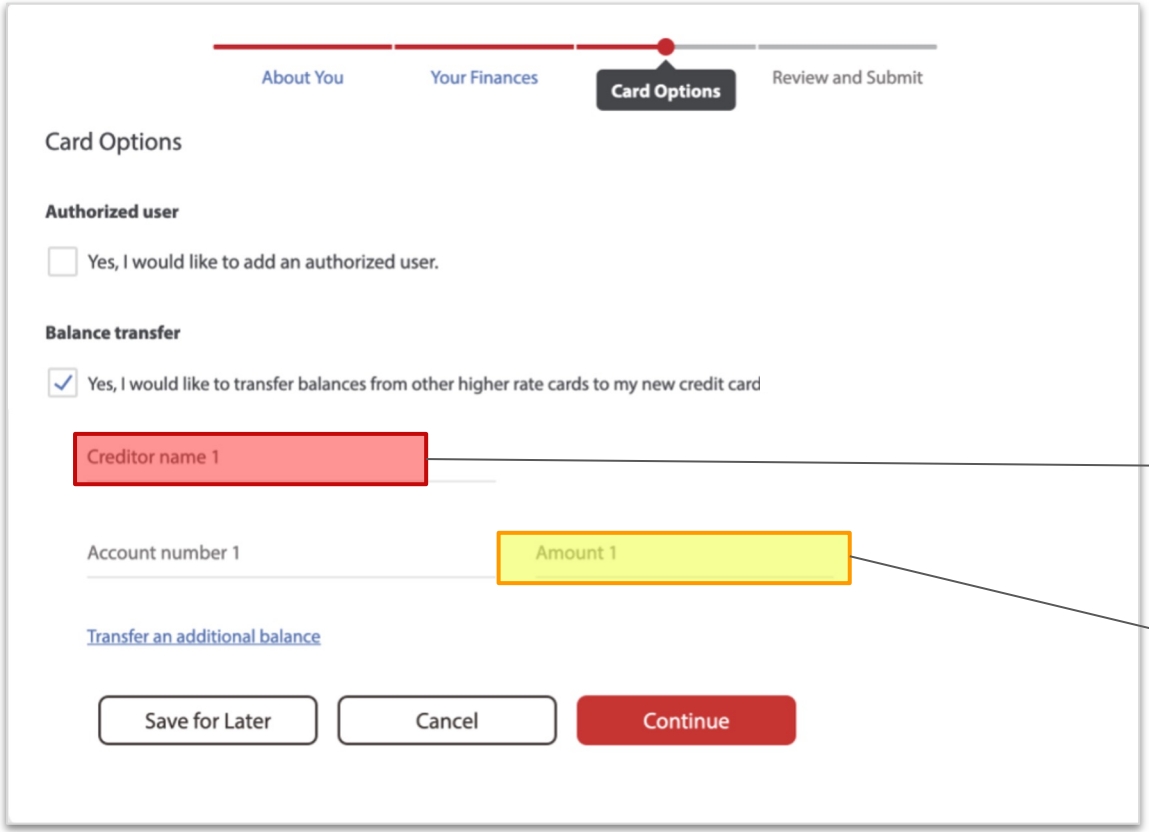


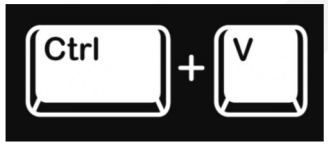
99% 0.4%

Pasting behavior
(Pasting on the Transfer Account Number fields)

USER BEHAVIOR

...and much more likely to paste in 'creditor name' and amount





More likely than good users to...

20x **Paste into 'Creditor name'**

40x **Paste into 'Amount'**

USER BEHAVIOR

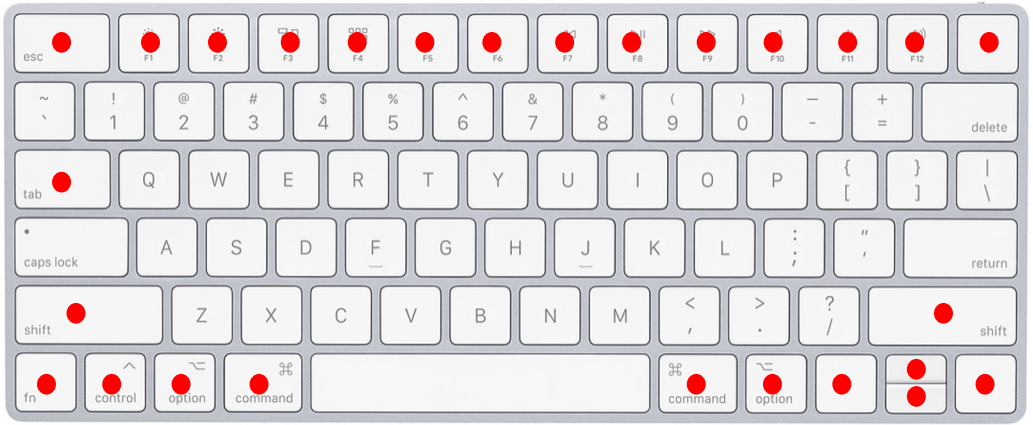
Fraudsters also tend to rely on keyboard shortcuts

Control/Command, option, function keys, arrows, etc

49%

0.6%

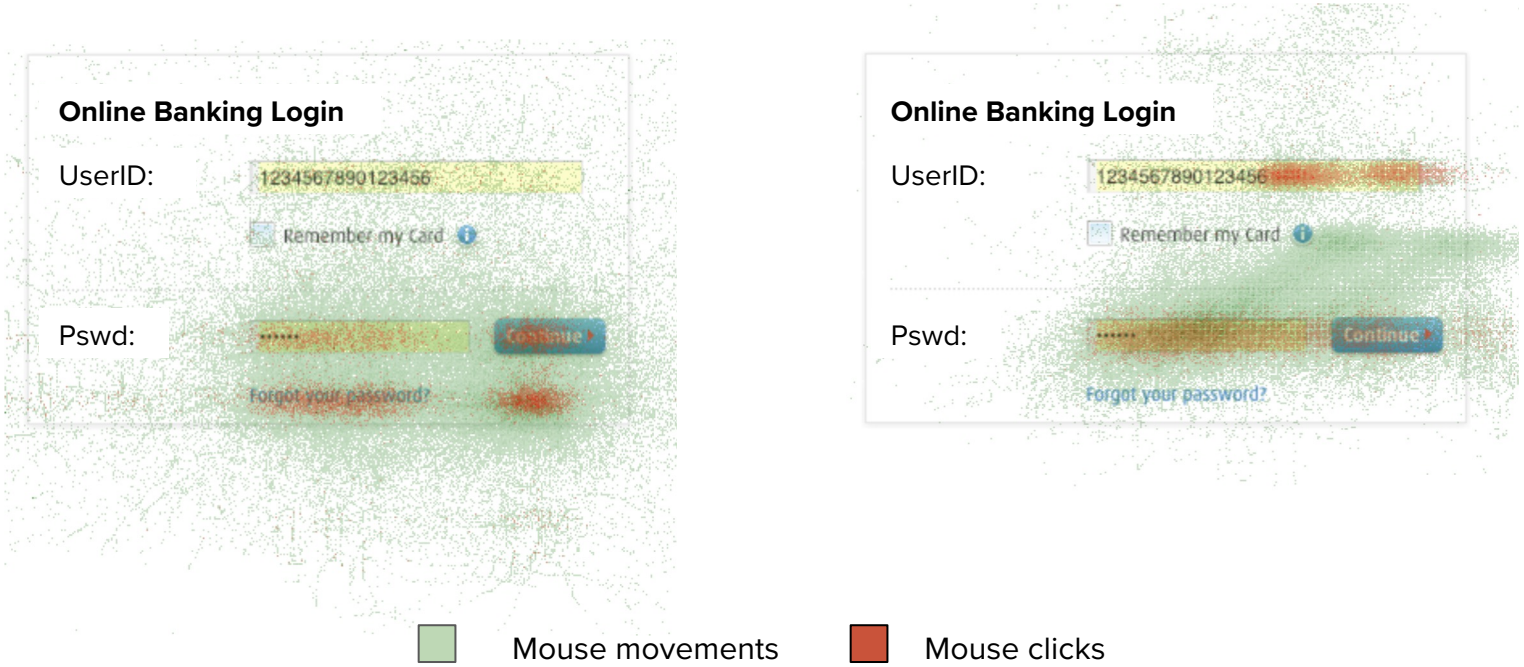
Unusual keys used



Fraud behavior is distinctive from legitimate users

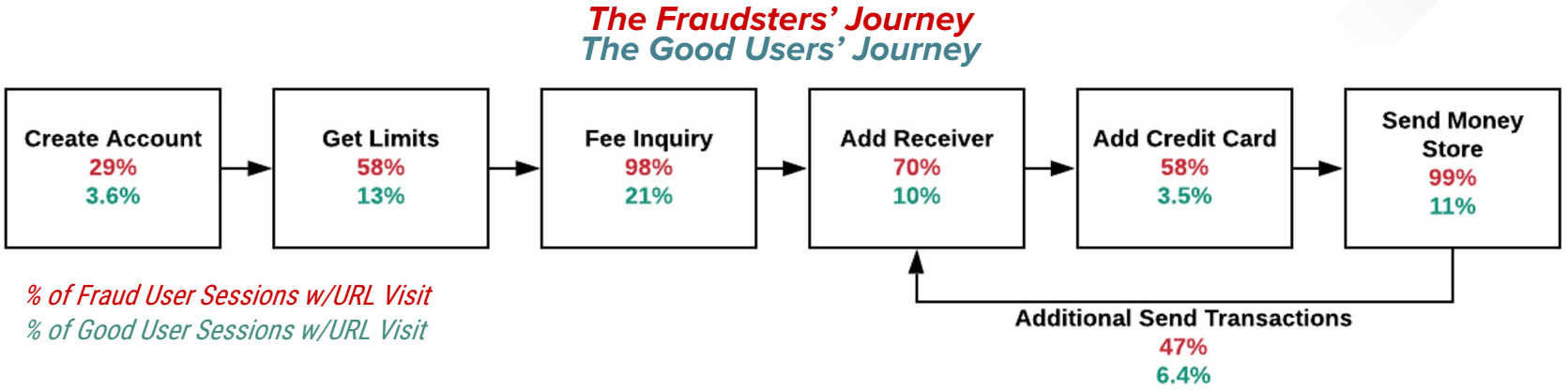
HOW

Humans are often clumsy and inefficient while fraudsters knows their way



Heat maps generated over 6,500 human and 6,500 fraudulent logins for a large North American bank.

Fraudsters navigate differently from good users



Money transfer sessions

***Fraud* sessions more likely to include:**

- New Account Creation
- Addition of New Receiver(s)
- Addition of New Credit Card(s)
- Sending Money to Multiple Receivers

***Good User* sessions more likely to include:**

- Funding transfer through a bank account
- Using a funding source already tied to the WU account

3

MFA only succeeds when it fails

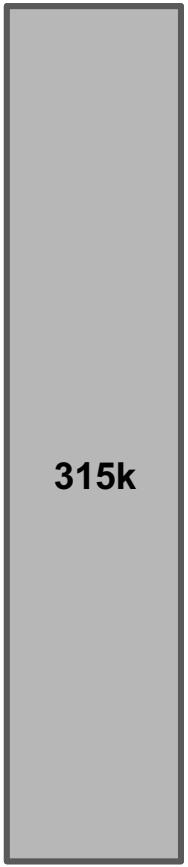
How well is your MFA strategy working?

(More friction authentication)

Standard metrics:
# of MFAs fired
# of MFAs fulfilled by users (pass)
# of MFAs not filled by user (block)

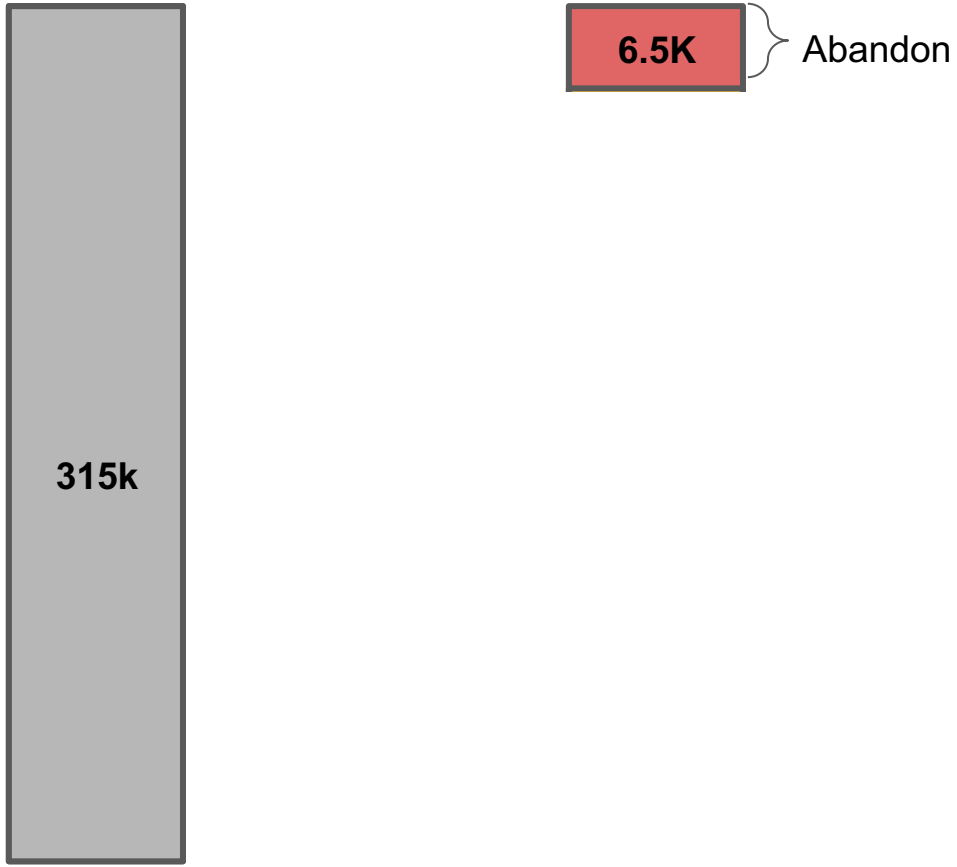
Contrarian metric:
MFAs fulfilled by users / MFAs fired
(this is the failure rate - and is the most important rate to measure)

Case study: Bank fired 315k MFAs on single day in May



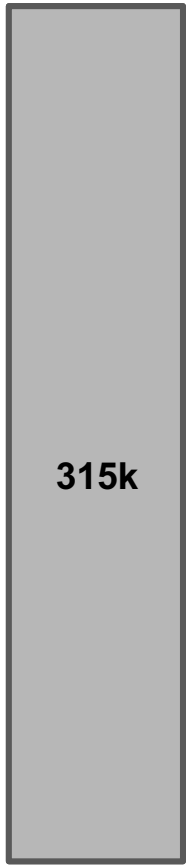
Either shown with permission, or replaced with a 1:1 direct equivalent company

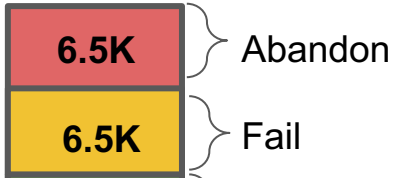
6,500 users, upon seeing MFA, simply abandoned process



Either shown with permission, or replaced with a 1:1 direct equivalent company

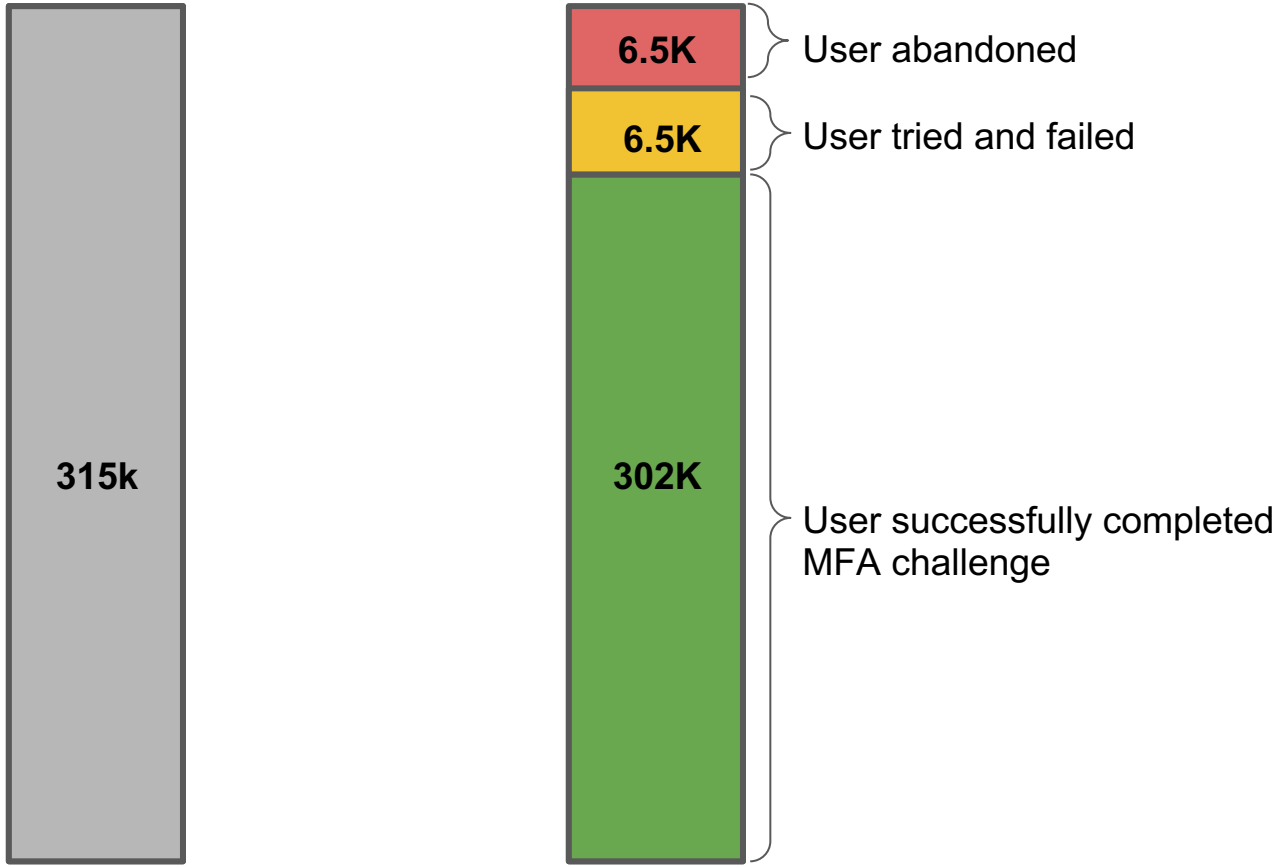
Another 6,500 tried to complete MFA and failed





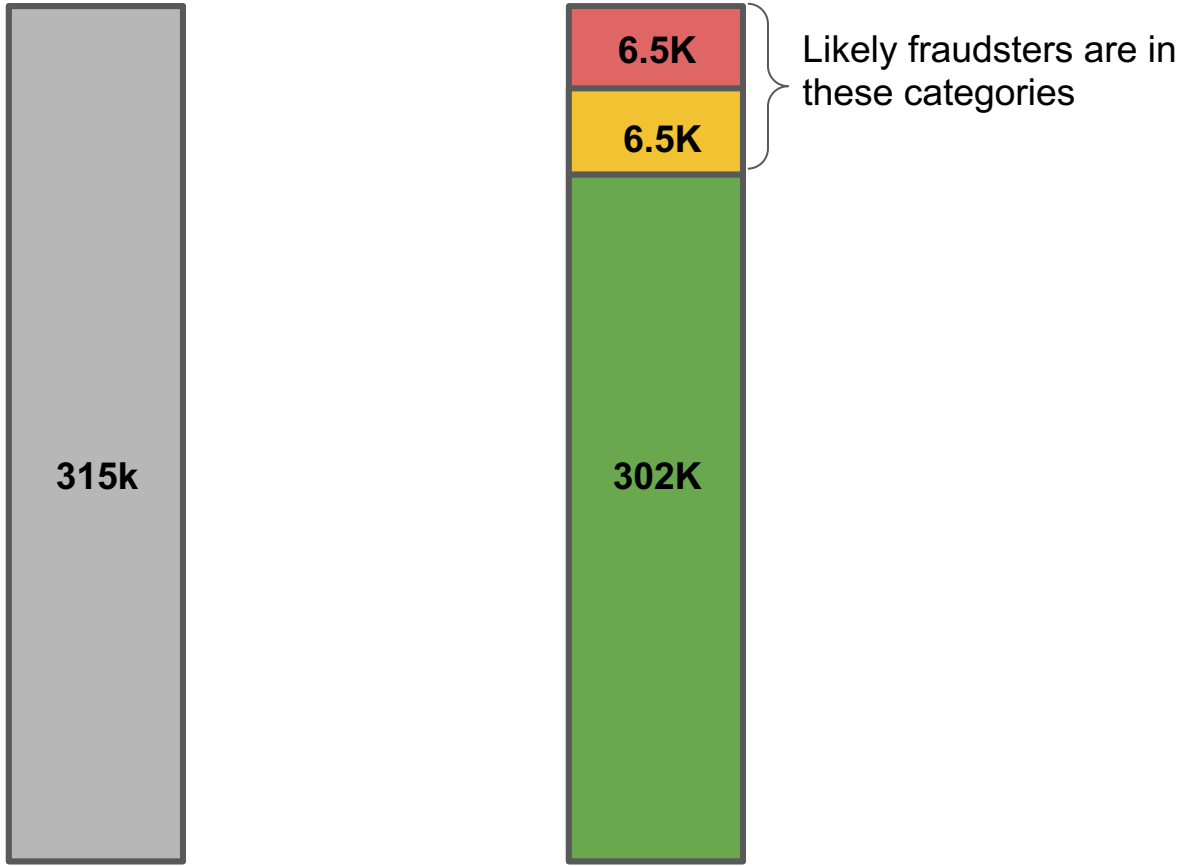
Either shown with permission, or replaced with a 1:1 direct equivalent company

302k out of 315k successfully completed MFA challenge



Either shown with permission, or replaced with a 1:1 direct equivalent company

Likely fraudsters are in red & yellow



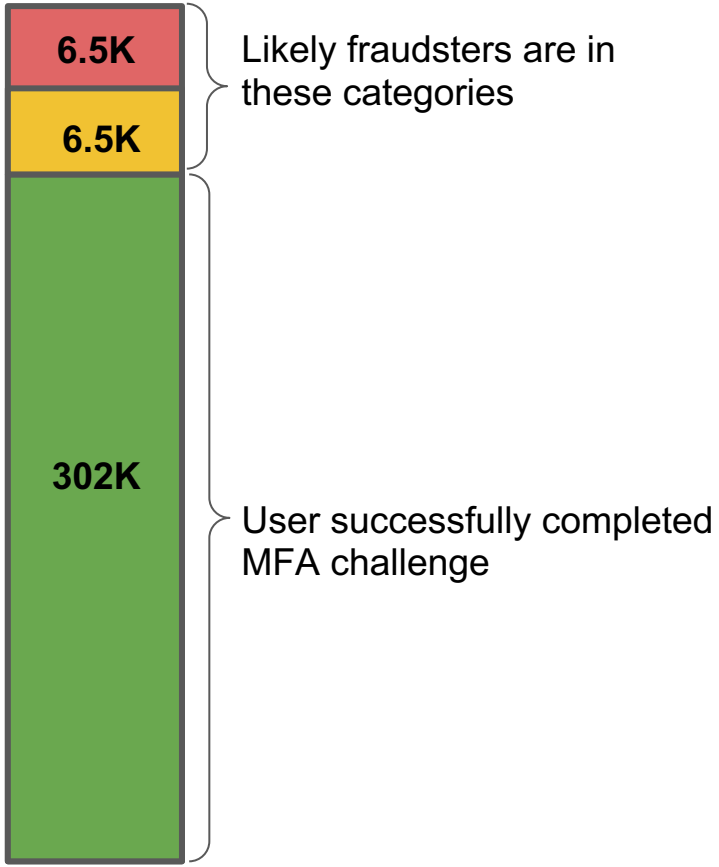
Either shown with permission, or replaced with a 1:1 direct equivalent company

~300k MFA challenges that were fulfilled = failures of fraud engine

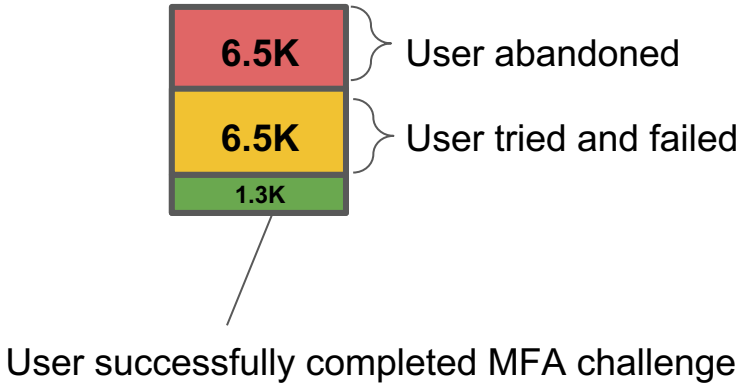
Vast majority of successfully completed MFAs represent needless friction for legitimate users

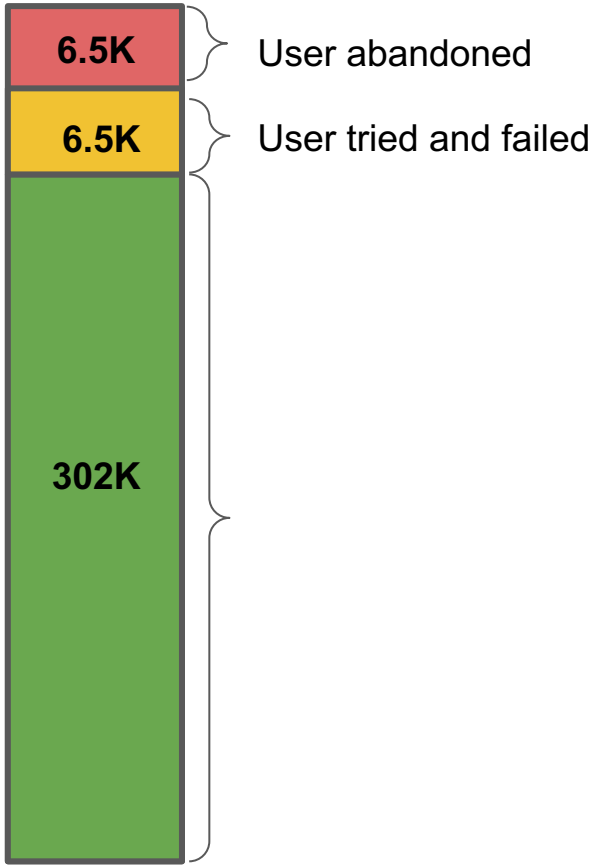
Over 95% of MFA challenges were issued to “wrong” users (i.e. legitimate users)

Success rate = 95%



Ideal ratio is about 10% successful completion of MFA





Two attributes of least-hated MFA:
-- in-app (i.e. Gmail uses in-app MFA inside GMail app)
-- no user pre-provisioning required (i.e. no device binding)

THANK YOU