Tracking the Use of Leaked Consumer Data

Tina Yeung & Dan Salsburg
OTech | FTC Office of Technology Research & Investigation
www.ftc.gov/OTech | research@ftc.gov

What Happens to Leaked Credentials?

Research question:

When consumer credentials are made public,

does anyone use them?

Goal:

Design and conduct a study that tracks the attempted use of stolen consumer credentials

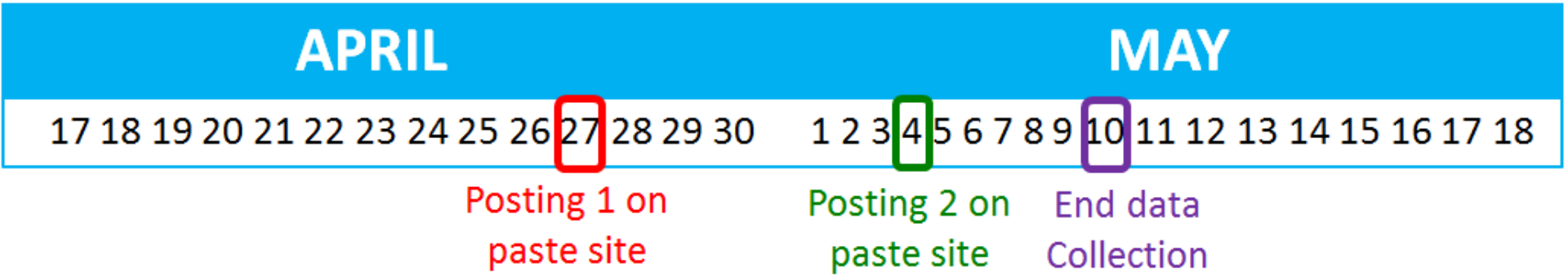
Study of Credential Use

1. Create ~100 consumer accounts
2. Post account data publicly
3. Track use of data

Fake Customer Data

1. Name
2. Address
3. Phone number
4. Email address
5. Password
6. Payment mechanism
    - Credit card number
    - Online payment account
    - Bitcoin wallet

Posting of Fake Customer Data



Posting One vs. Posting Two

- Same data, posted twice
- Different format and time of day

Posting 1: ~100 views

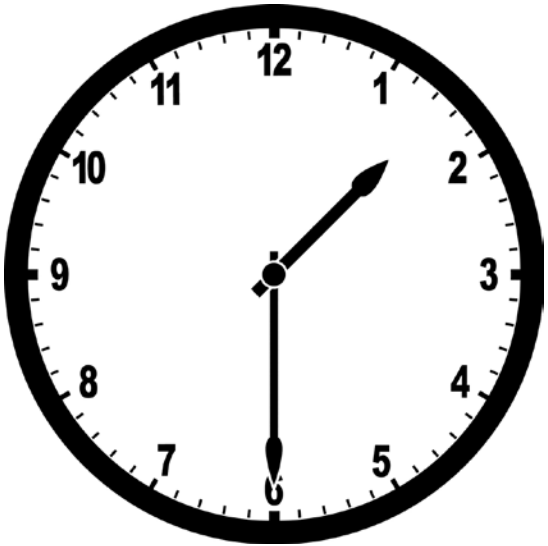
Posting 2: ~550 views
(Picked up by Twitter bot)

Monitoring of Data Usage

- Monitored for about three weeks
  - Week before Posting 1 (Pre-study control)
  - Week after Posting 1 (Week 1)
  - Week after Posting 2 (Week 2)
- Logged
  - Email account access attempts
  - Payment account access attempts
  - Credit card attempted charges
  - Texts and calls received by phone numbers

Time Before First Unauthorized Access Attempt

Posting 1

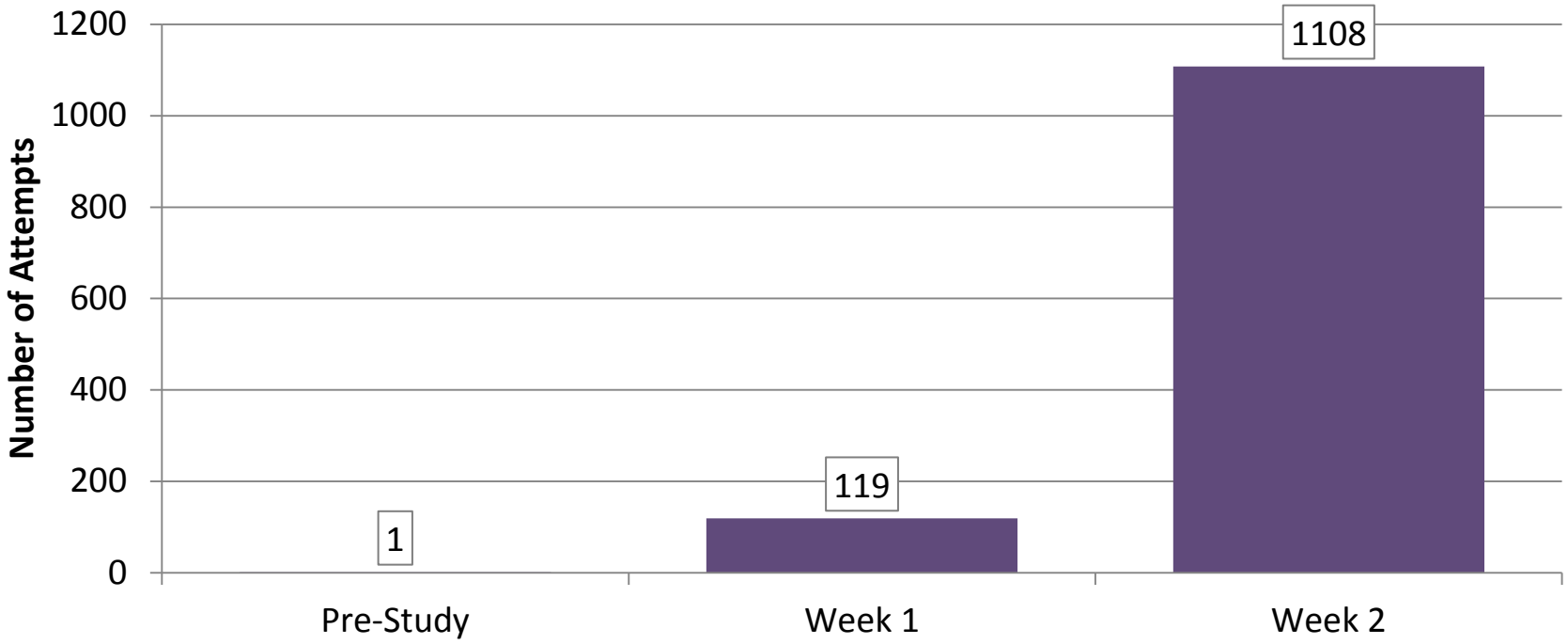


1.5 hours

Posting 2

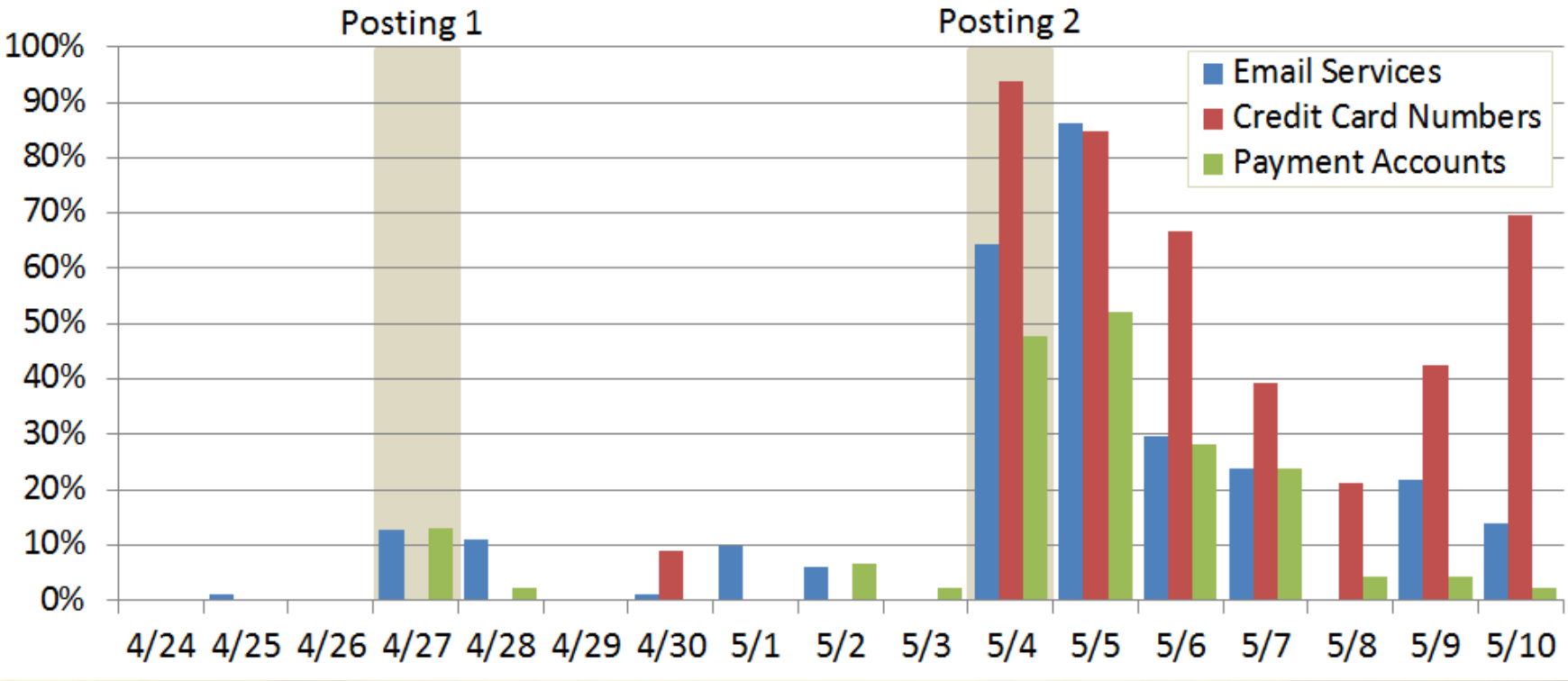
9 minutes

Total Unauthorized Access Attempts



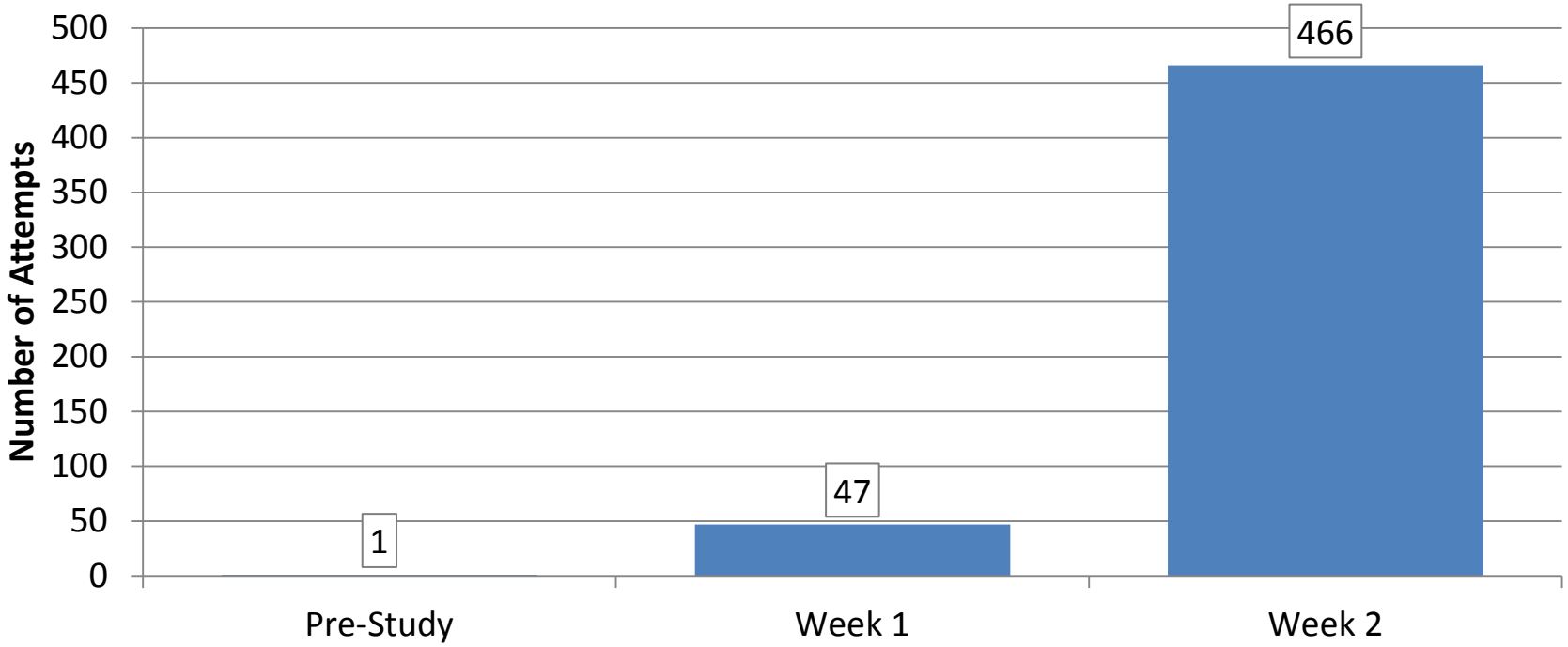
Unauthorized Access Attempts by Account Type

Account Activity

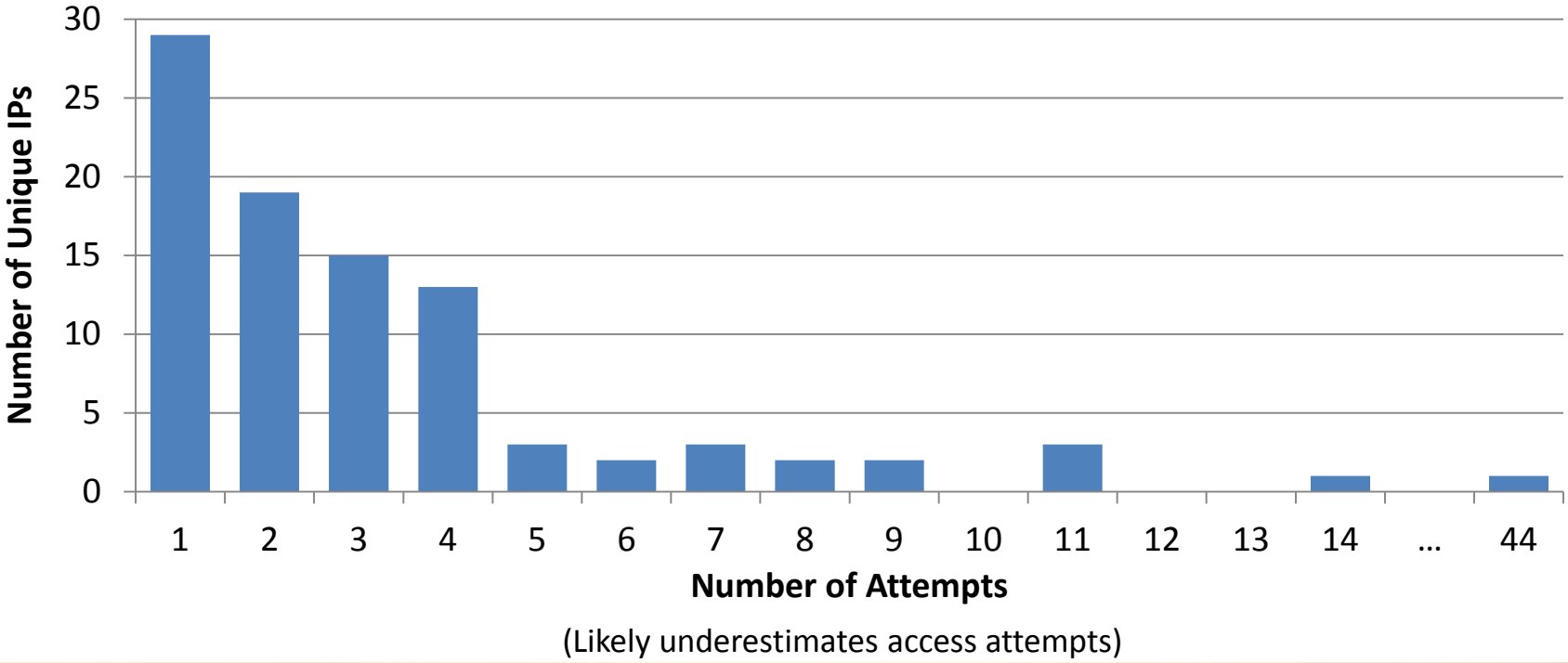


#IDTheftFTC

Email Account Access Attempts by Week

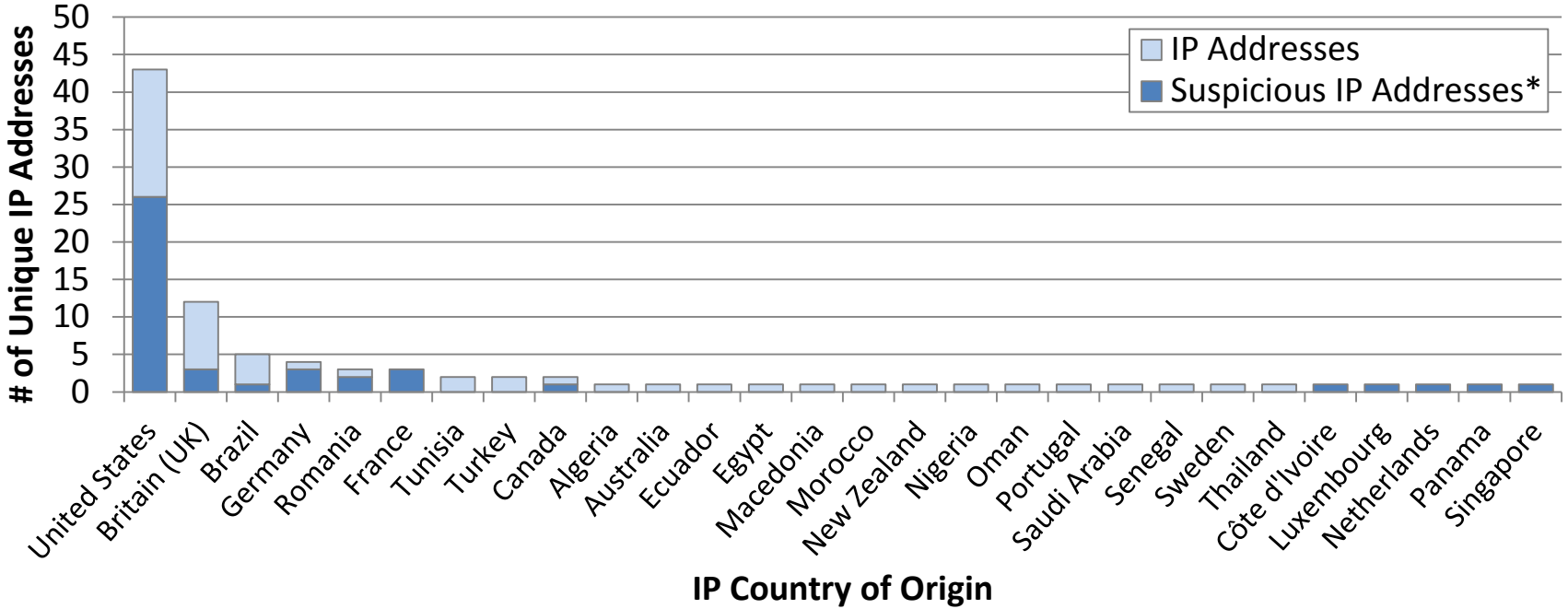


Email Access Attempts by Unique IP Addresses



(Likely underestimates access attempts)

Geolocation of IPs Used in Access Attempts

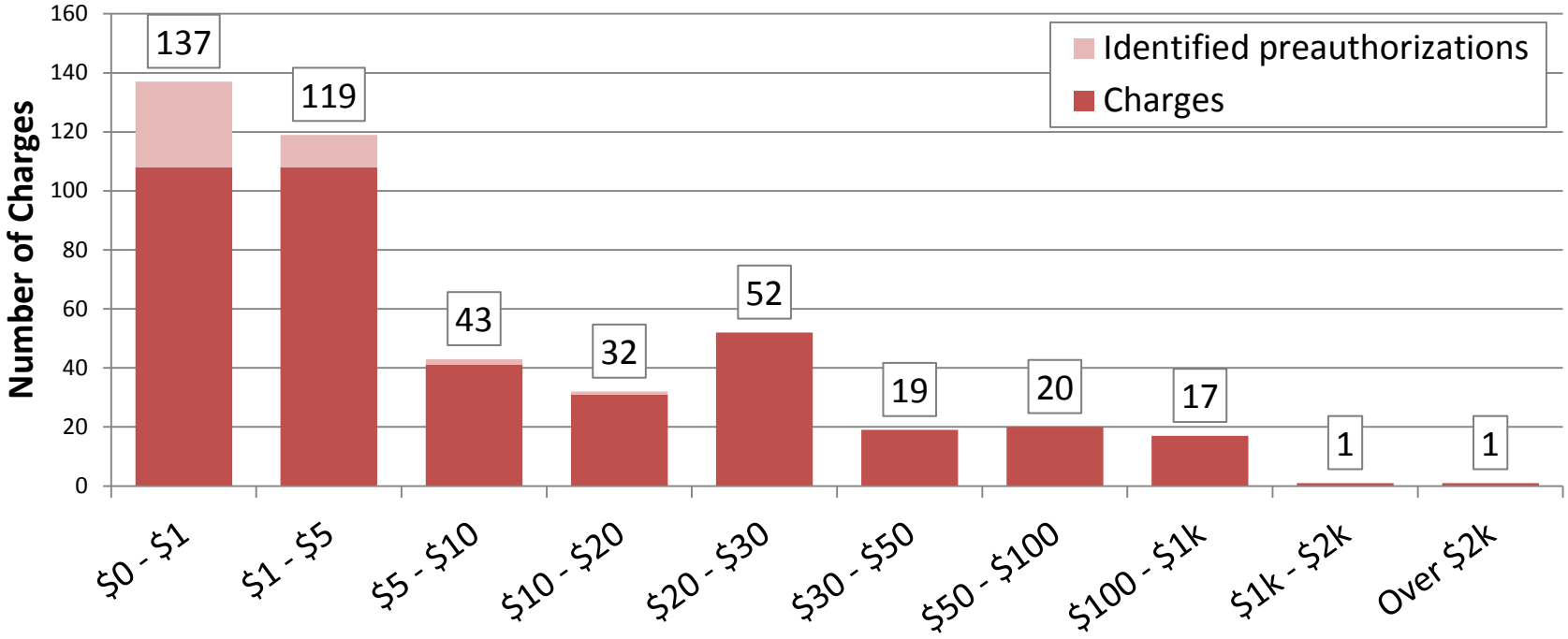


*IP addresses identified as suspicious by a freely available service

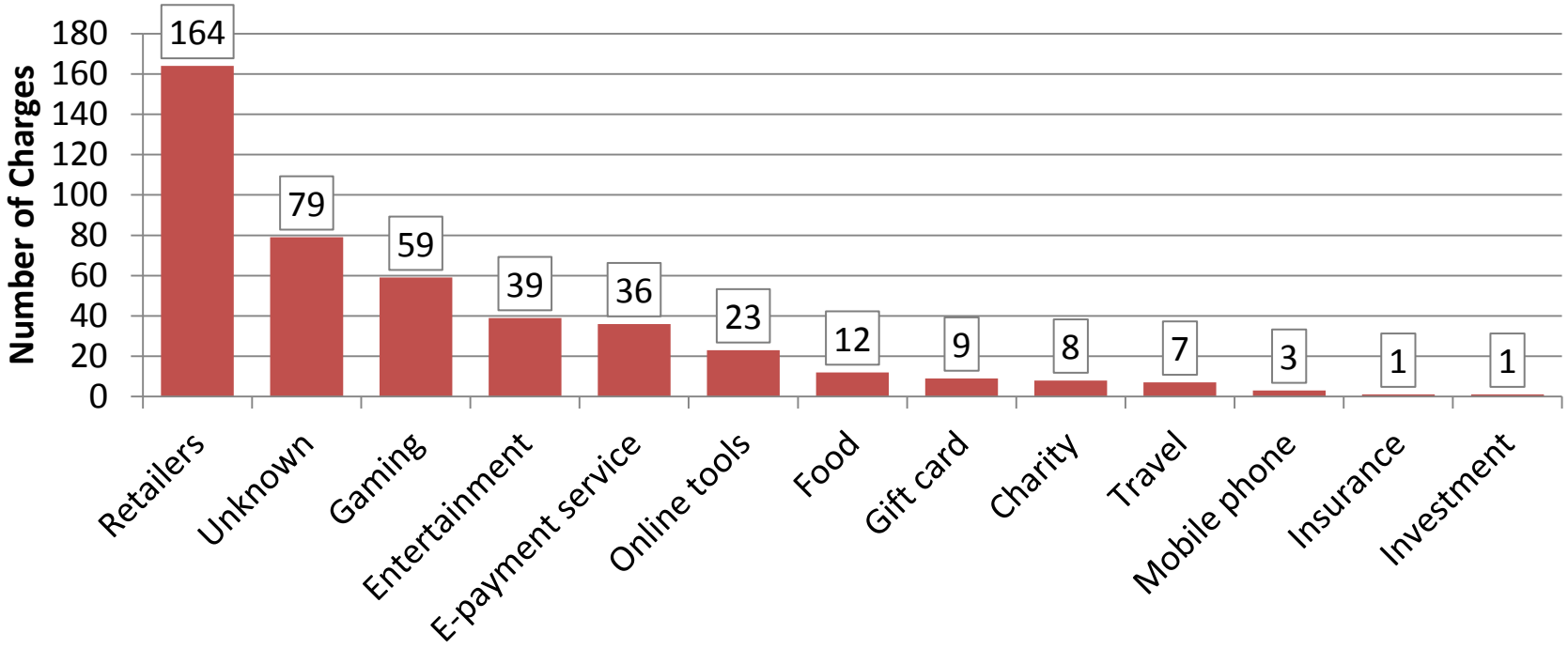
Credit Card Purchase Attempts

- Max: $2,697.75, at a clothing website
- Total amount within two weeks: $12,825.53
  - Includes multiple payment attempts
  - Includes preauthorization charges
- Noteworthy attempts:
  - Online dating service
  - Pizza place
  - Hotels

Amount Attempted per Charge



Charge by Category



Additional Thoughts

- If you post it, they will use it
- Paste sites should be monitored by email and payment service providers
- Two factor authentication provides some protection against stolen credentials
- Merchants should consider refusing seriatim purchase attempts

Future work

- Analysis of email spam, text spam, and phone calls received by fake consumer email accounts
- Posting of consumer data in other ways that might attract different types of thieves

Have relevant research?

www.ftc.gov/OTech | research@ftc.gov

Contributors

- Sheryl Roth
- Phoebe Rouge
- Joe Calandrino
- Aaron Alva
- Justin Brookman
- Phillip Miyo
- Nicole Davis
- Aaron Kaufman
- Amber Howe
- Biaunca Morris
- Jonathan Aid
- Anne Blackman