Preventative Approaches to DNS Abuse Mitigation

DNS Abuse Institute

Preventative vs. Reactive

- Reactive: Ry/Rr receives report of abuse, investigates, mitigates
- Preventative: Detecting *potentially* malicious domains before registration or resolution
- Trade off in costs and business impacts

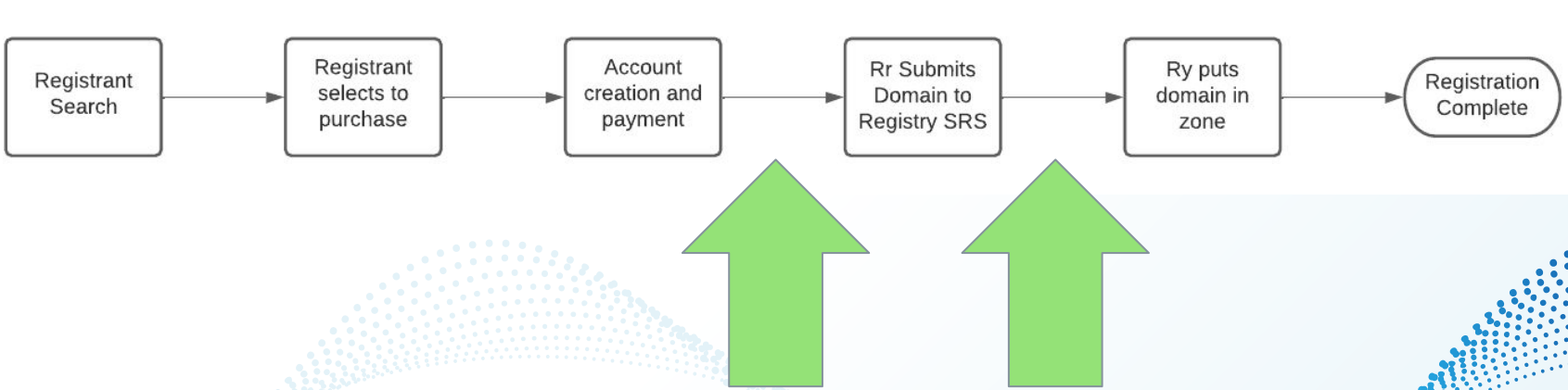
Detection at what level?

- Ry: Can apply detection across an entire zone, limited information, requires Rr intermediary
- Rr: More information, customer relationship, variety of implementations

Incentives are Key

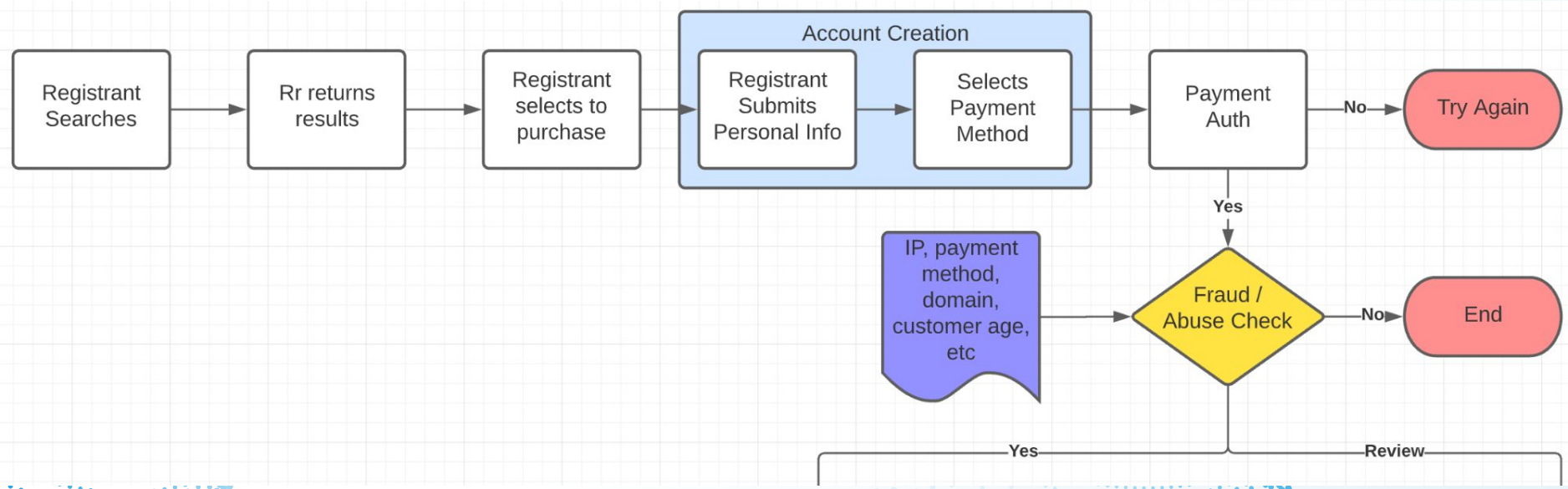
- Preventive methods require friction in the registration process
- Requires scarce & expensive engineering resources
- Need to demonstrate:
  - Lowers costs
  - Little/no impact on revenue

Domain Registration Process



DNS ABUSE INSTITUTE

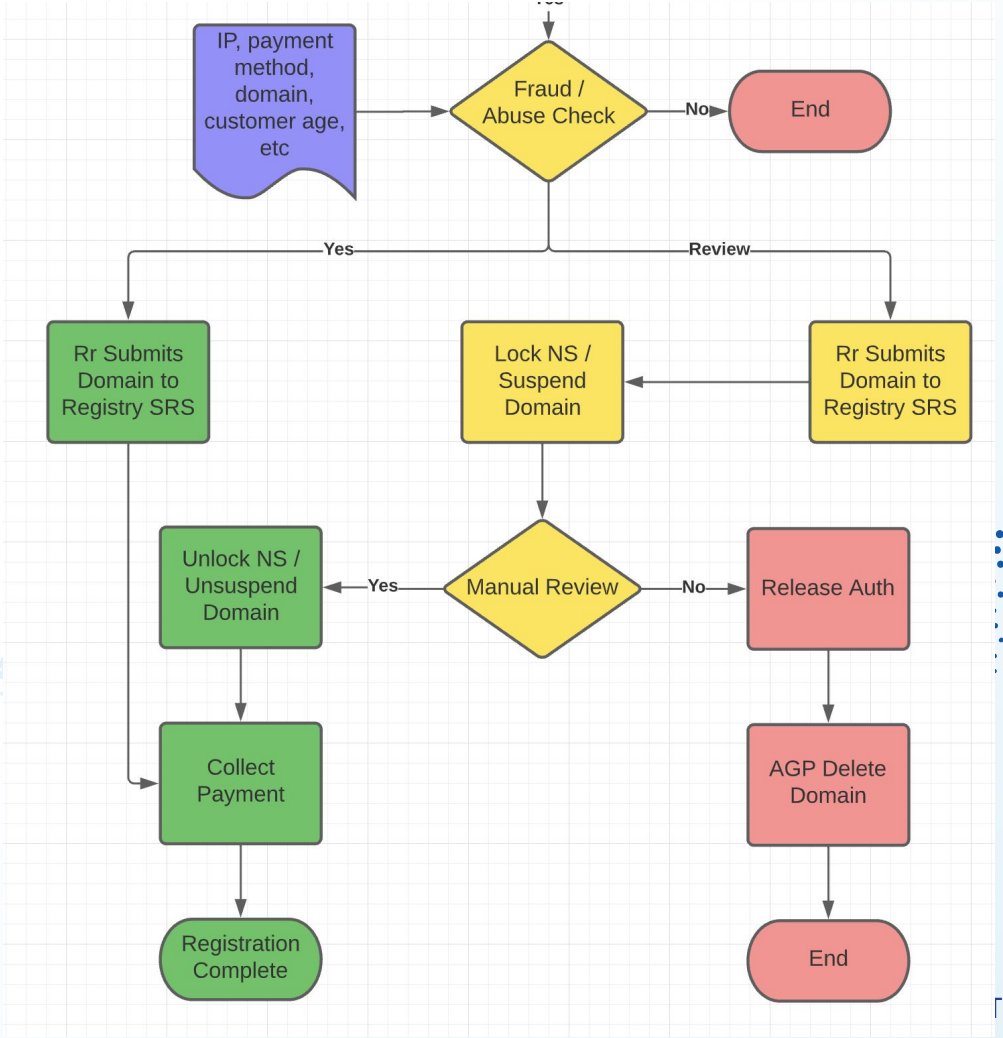
Part 1:Leveraging Fraud Detection



DNS ABUSE INSTITUTE

Optimal Flow

- Leverage and optimise existing fraud tools
- Limit harms by suspending review queue



To Do

- Identify the most important transactional attributes
- Identify most common payment processors
- Tune weights
- Globalize learnings
- Share results

Questions?

Graeme Bunton

@graemebunton

graeme@dnsabuseinstitute.org

DNS ABUSE INSTITUTE