MESSAGING MALWARE MOBILE ANTI-ABUSE WORKING GROUP

Economics of Abuse Operations: Application to Hosting

Matthew C. Stith

September 28, 2016

San Jose, Costa Rica

About the presenter

- 8 Years at Rackspace
- Rackspace's Acceptable Use Team and Postmaster
- Co-Chair of M3AAWG's Hosting Committee
- Member of M3AAWG's Board of Directors

History of Rackspace Anti-Abuse Teams

- The beginning
- Lessons learned
- Change in the landscape and team
- The Future

In the beginning there was spam

- Rackspace was founded in 1998 but did not have an Acceptable Use Policy or AUP team until 2000
  - Reports that Rackspace was a haven for child exploitation and spammers was published
  - Law enforcement contacted Rackspace about the existence of child exploitation
  - Acceptable Use Policy was written and a team formed

MESSAGING MALWARE MOBILE ANTI-ABUSE WORKING GROUP

More Spam and Buyin from Above

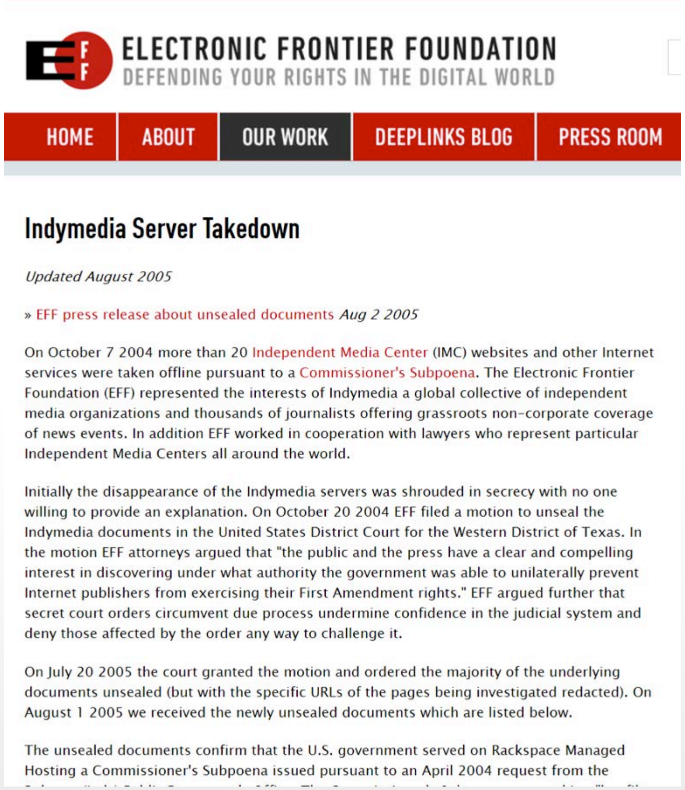
- The "Spammer Special"
- Skylist (2002)
  - Rackspace's first 1 million dollar customer
  - Was a notorious spammer
  - Became listed on Spamhaus' ROSKO list 2003
  - An entire new datacenter was all blacklisted
- Rackspace leadership made the decision to terminate Skylist
- Along with the passage of the CAN-SPAM

A lesson in enforcement

M3AAWG
Messaging Malware Mobile Anti-Abuse Working Group

- Rackspace received its first Law Enforcement request in 2004 for Indymedia
- On the advice of counsel we contacted the FBI and did everything that they said.

It did not go well


ELECTRONIC FRONTIER FOUNDATION
DEFENDING YOUR RIGHTS IN THE DIGITAL WORLD
HOME
ABOUT
OUR WORK
DEEPLINKS BLOG
PRESS ROOM

Indymedia Server Takedown

Updated August 2005

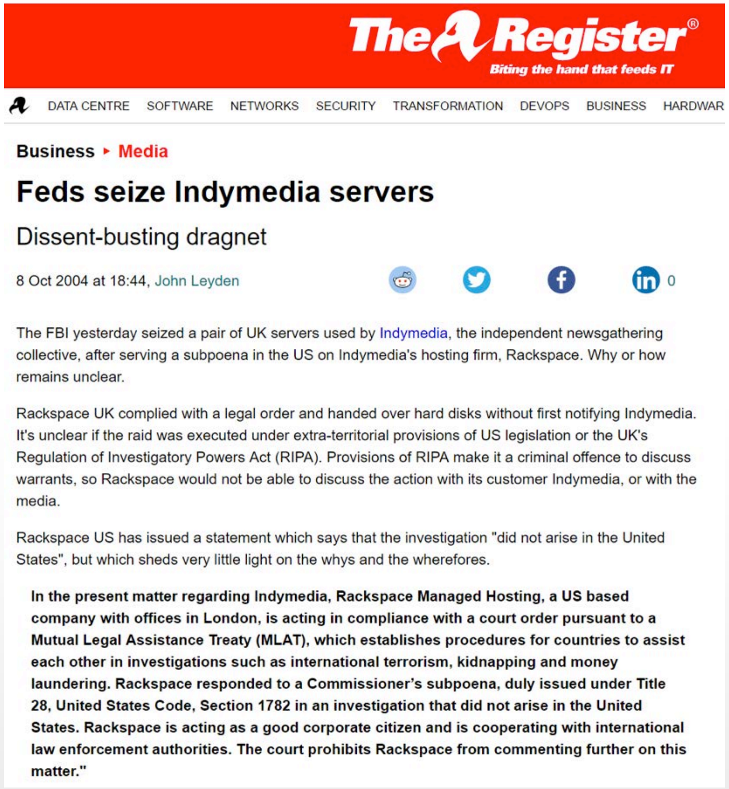
» EFF press release about unsealed documents *Aug 2 2005*

On October 7 2004 more than 20 Independent Media Center (IMC) websites and other Internet services were taken offline pursuant to a Commissioner's Subpoena. The Electronic Frontier Foundation (EFF) represented the interests of Indymedia a global collective of independent media organizations and thousands of journalists offering grassroots non-corporate coverage of news events. In addition EFF worked in cooperation with lawyers who represent particular Independent Media Centers all around the world.

Initially the disappearance of the Indymedia servers was shrouded in secrecy with no one willing to provide an explanation. On October 20 2004 EFF filed a motion to unseal the Indymedia documents in the United States District Court for the Western District of Texas. In the motion EFF attorneys argued that "the public and the press have a clear and compelling interest in discovering under what authority the government was able to unilaterally prevent Internet publishers from exercising their First Amendment rights." EFF argued further that secret court orders circumvent due process undermine confidence in the judicial system and deny those affected by the order any way to challenge it.

On July 20 2005 the court granted the motion and ordered the majority of the underlying documents unsealed (but with the specific URLs of the pages being investigated redacted). On August 1 2005 we received the newly unsealed documents which are listed below.

The unsealed documents confirm that the U.S. government served on Rackspace Managed Hosting a Commissioner's Subpoena issued pursuant to an April 2004 request from the



Business ▸ Media

Feds seize Indymedia servers

Dissent-busting dragnet

8 Oct 2004 at 18:44, John Leyden

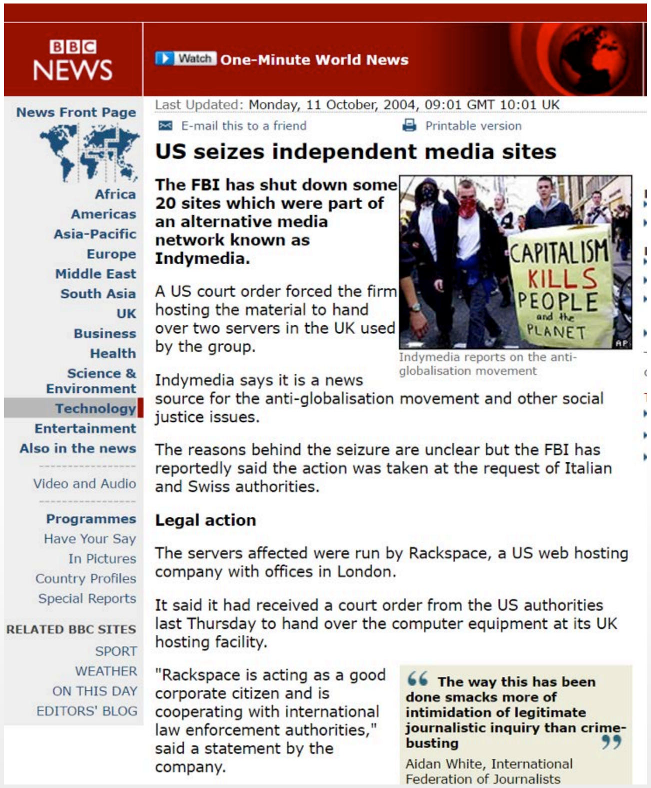
The FBI yesterday seized a pair of UK servers used by Indymedia, the independent newsgathering collective, after serving a subpoena in the US on Indymedia's hosting firm, Rackspace. Why or how remains unclear.

Rackspace UK complied with a legal order and handed over hard disks without first notifying Indymedia. It's unclear if the raid was executed under extra-territorial provisions of US legislation or the UK's Regulation of Investigatory Powers Act (RIPA). Provisions of RIPA make it a criminal offence to discuss warrants, so Rackspace would not be able to discuss the action with its customer Indymedia, or with the media.

Rackspace US has issued a statement which says that the investigation "did not arise in the United States", but which sheds very little light on the whys and the wherefores.

> **In the present matter regarding Indymedia, Rackspace Managed Hosting, a US based company with offices in London, is acting in compliance with a court order pursuant to a Mutual Legal Assistance Treaty (MLAT), which establishes procedures for countries to assist each other in investigations such as international terrorism, kidnapping and money laundering. Rackspace responded to a Commissioner's subpoena, duly issued under Title 28, United States Code, Section 1782 in an investigation that did not arise in the United States. Rackspace is acting as a good corporate citizen and is cooperating with international law enforcement authorities. The court prohibits Rackspace from commenting further on this matter."**

It did not go well



Last Updated: Monday, 11 October, 2004, 09:01 GMT 10:01 UK

US seizes independent media sites

The FBI has shut down some 20 sites which were part of an alternative media network known as Indymedia.

A US court order forced the firm hosting the material to hand over two servers in the UK used by the group.

Indymedia reports on the anti-globalisation movement

Indymedia says it is a news source for the anti-globalisation movement and other social justice issues.

The reasons behind the seizure are unclear but the FBI has reportedly said the action was taken at the request of Italian and Swiss authorities.

Legal action

The servers affected were run by Rackspace, a US web hosting company with offices in London.

It said it had received a court order from the US authorities last Thursday to hand over the computer equipment at its UK hosting facility.

"Rackspace is acting as a good corporate citizen and is cooperating with international law enforcement authorities," said a statement by the company.

> **The way this has been done smacks more of intimidation of legitimate journalistic inquiry than crime-busting**
>
> Aidan White, International Federation of Journalists

The Rise of "THE CLOUD"

M3AAWG
Messaging Malware Mobile Anti-Abuse Working Group

- Fast forward to 2008
  - Kicking spammers off the network
  - Preventing exploitation on network
  - Proper processes for customers and the business
  - Then suddenly….. The cloud
    - Within months spam complaints became hacking complaints
    - Fraud…. So much fraud

      Poor controls, no limits

      Customers getting IPs that were already tainted

The future

- Data Driven Approaches
- Automate
- Integration with product organizations

Putting an abuse desk into perspective

M3AAWG
Messaging Malware Mobile Anti-Abuse Working Group

- Protecting the system
  - Being on the internet makes your company a target for abuse
  - No one customer is bigger than the whole system
  - Pay attention to outliers
- Protecting the customer
  - Users are your weakest point of defense
  - Customers depend on the service to be up
  - Deter malicious parties from considering your service
  - Know about issues with customers before they do

Compromises

- Customer services and accounts
  - Support
  - Remediation
  - Downtime of customer/system environments
- Customers attacking other customers
  - Gives the appearance of lack of security
  - Having to play both sides of the fence (complainer and complainant)
- Knowledge of when and how to suspend/terminate

Attacks

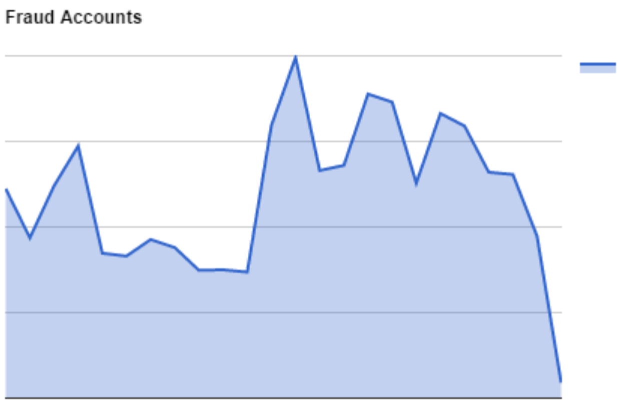
M3AAWG
Messaging Malware Mobile
Anti-Abuse Working Group

- Phishing campaigns on customers and employees
  - Theft of information
    - Personal
    - Financial
    - Company Specific
- DDOS
  - Misconfigurations
  - Retaliation
- Hacking
  - Brute force
  - Defaced sites / Malware payloads

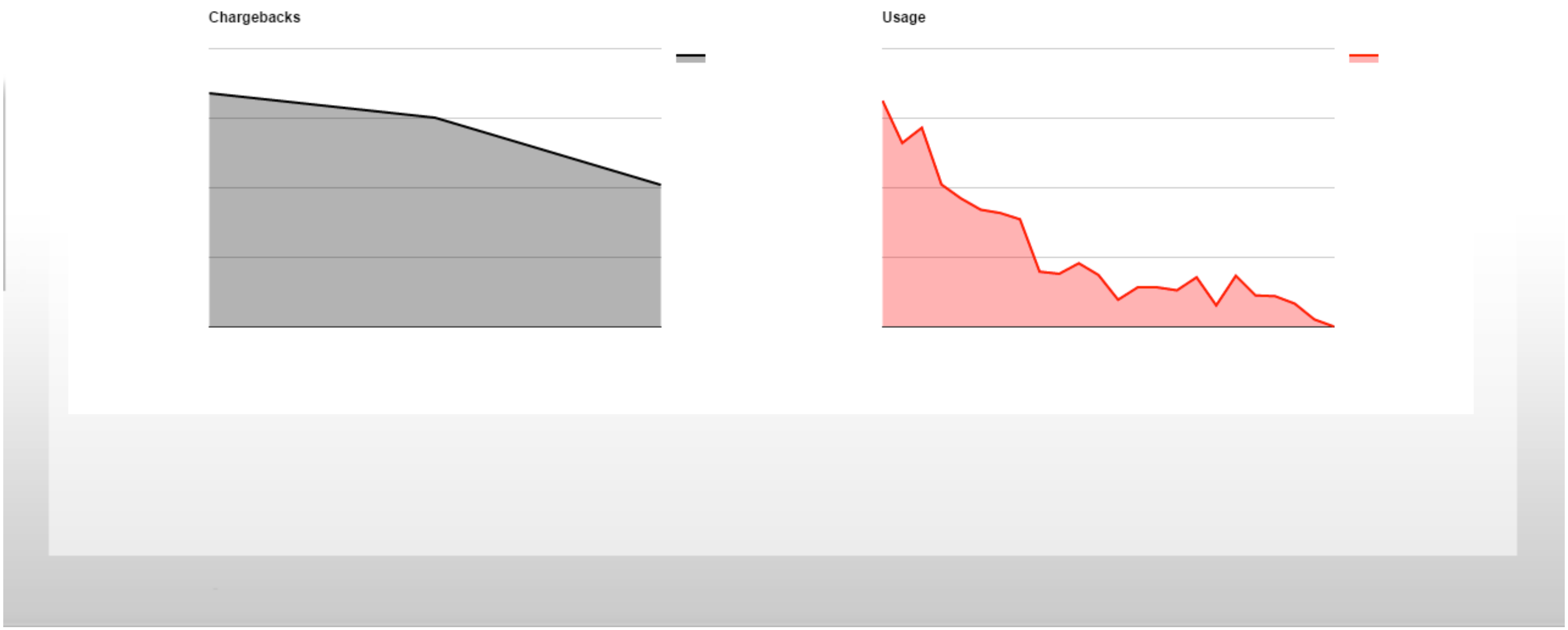
Fraud

- Impacts profitability
  - Chargebacks
  - Revenue loss from usage
- Network issues
  - IP and domain blacklisting
  - Over utilization of resources
- Support overhead
  - Accounts receivable
  - Support being abused

Fraud Trends Cloud

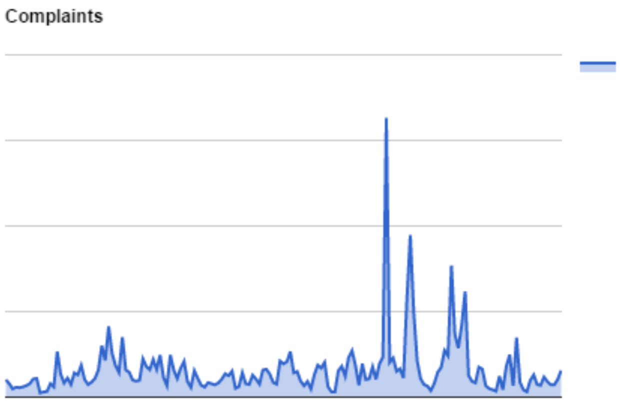


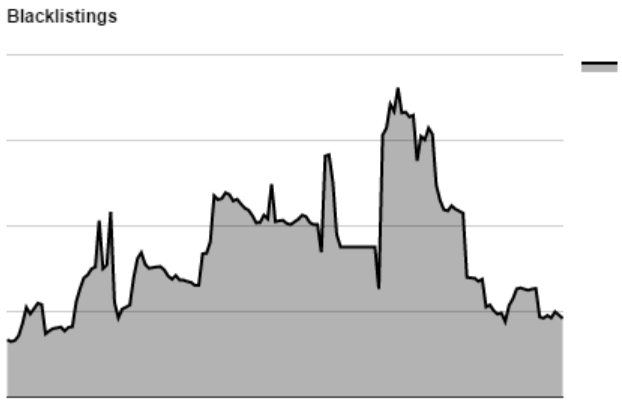
Fraud Trends Cloud



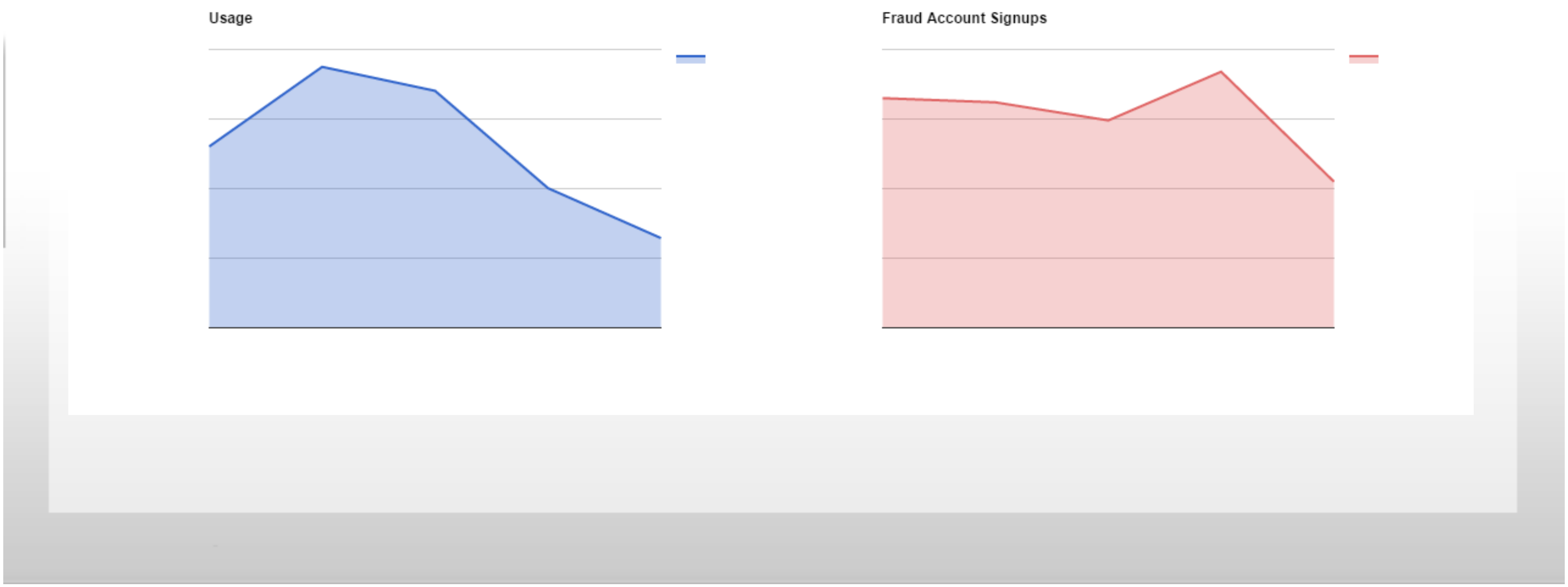
Fraud Trends Email

M3AAWG
Messaging Malware Mobile
Anti-Abuse Working Group





Fraud Trends Email



Industry Expertise and Partnerships

M³AAWG
MESSAGING MALWARE MOBILE
ANTI-ABUSE WORKING GROUP

- The landscape can change rapidly
- Training of staff and customers
- Gaining and sharing knowledge
  - Certifications
  - Trusted reporters and contacts
  - Industry specific groups
- Faster remediation of issues impacting your network from outside sources

A word on headcount

M3AAWG
Messaging Malware Mobile
Anti-Abuse Working Group

- “I’ll just ask for a team of 20 people to fight all of this!”
- Start small aim for what impacts your system the most
- Gather data
  - Customer downtime due to abuse
  - Loss of revenue
  - Blacklistings
  - Compromises/Fraud
  - Overall complaints and type
- Grow organically
  - Know what kind of worker you are looking for
  - Sometimes head count isn’t the answer