**Bones Society of Florida**

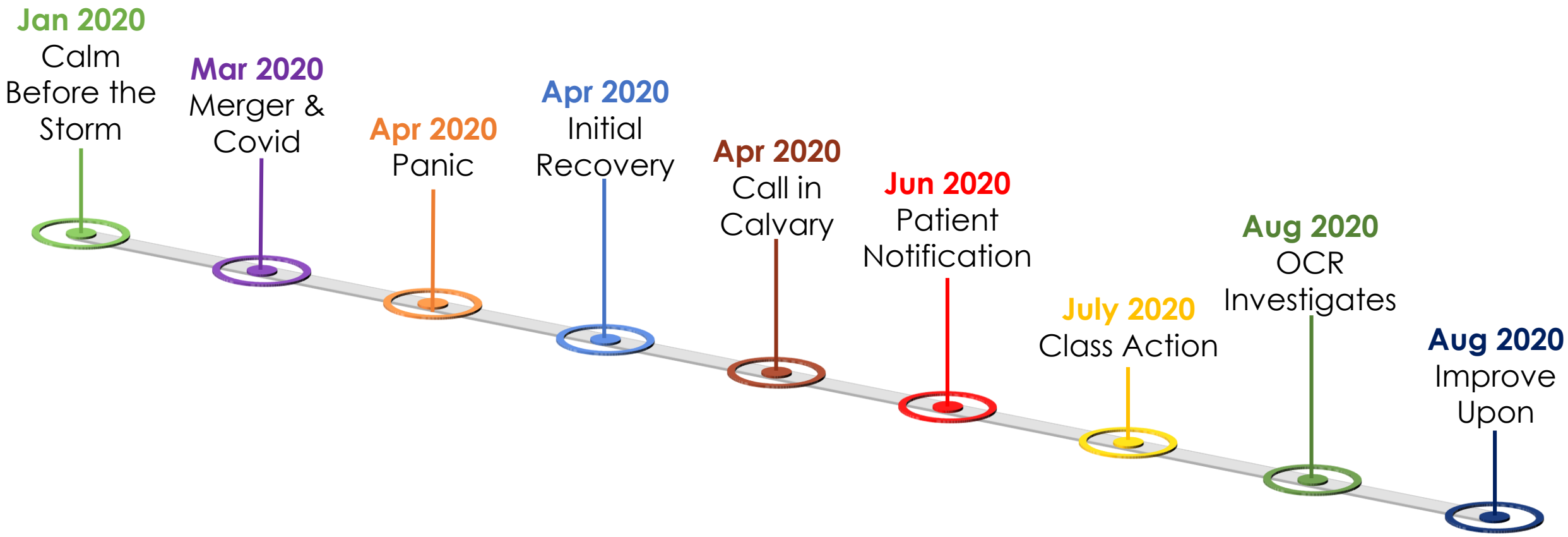
March, 2023

# Ransomware Attacks are not HUMERUS!

## *The insiders view on a network compromise and recovery*

FLORIDA ORTHOPAEDIC INSTITUTE®

# The Year of 2020 at FOI




FLORIDA ORTHOPAEDIC INSTITUTE

# Jan 2020 – The Calm Before The Storm

***How do you prepare for Ransomware?***

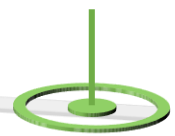
- Tighten security controls
- Limit access
- 2 factor everything

***How do you prepare for Litigation and Audits?***

- Document improvements to security
- Document the reason you are not doing other security improvements
- Discuss completed and in-flight security projects at board meetings
- Be careful on your wording when talking about future security plans

**Lesson's Learned**

1. Start Today
2. Cautiously document meeting minutes
3. Email, Text, IM, Paper, and Recordings can all be used in discovery



# Mar 2020 – Merger / COVID

***What was occurring at our Practice during this time?***

- March 2, 2020 – Merged with large practice in adjacent counties which doubles the size of our organization
- March 20, 2020 – Governor issues executive order 20-72; Non-essential Elective Medical Procedures
- March 23, 2020 – Physician tests positive for COVID and was in multiple locations; ultimately 10 locations including our main location were closed for a week
- Rapid deployment of work from home strategy ensues

**Lesson's Learned**

1. Disaster Planning
2. Training




FLORIDA ORTHOPAEDIC INSTITUTE

# Apr 2020 – Panic

***How did this attacker get access?***

- 3/28/2020 – Intrusion into the network using valid credentials over a VPN to a remote desktop
- 4/6/2020 – Attempt to exfiltrate patient data
- 4/8/2020 – Ransomware deployed to all computers and servers
- 4/9/2020 – 182 servers, 756 workstations ransomed

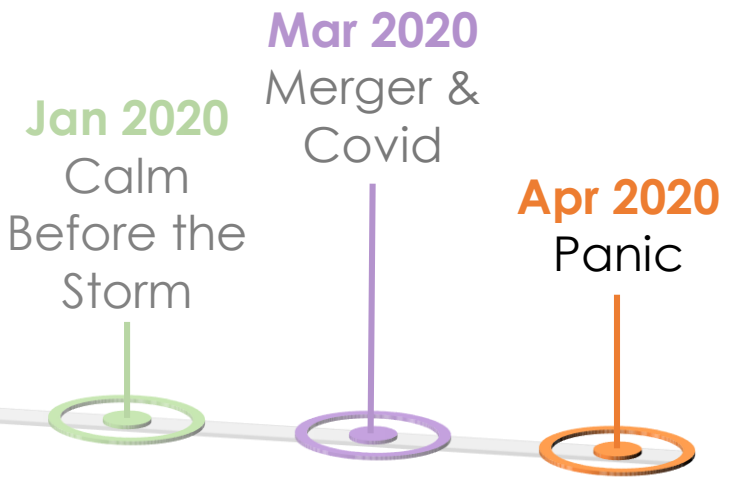
***What does ransomware look like to a practice?***

- PACS inaccessible, File shares encrypted, Phones inoperable
- Internet inaccessible from corporate computers
- Users panicking
- Full shutdown of all systems authorized, disable network links

**Lesson's Learned**

1. Have a triage list of what applications are most critical to patient care.

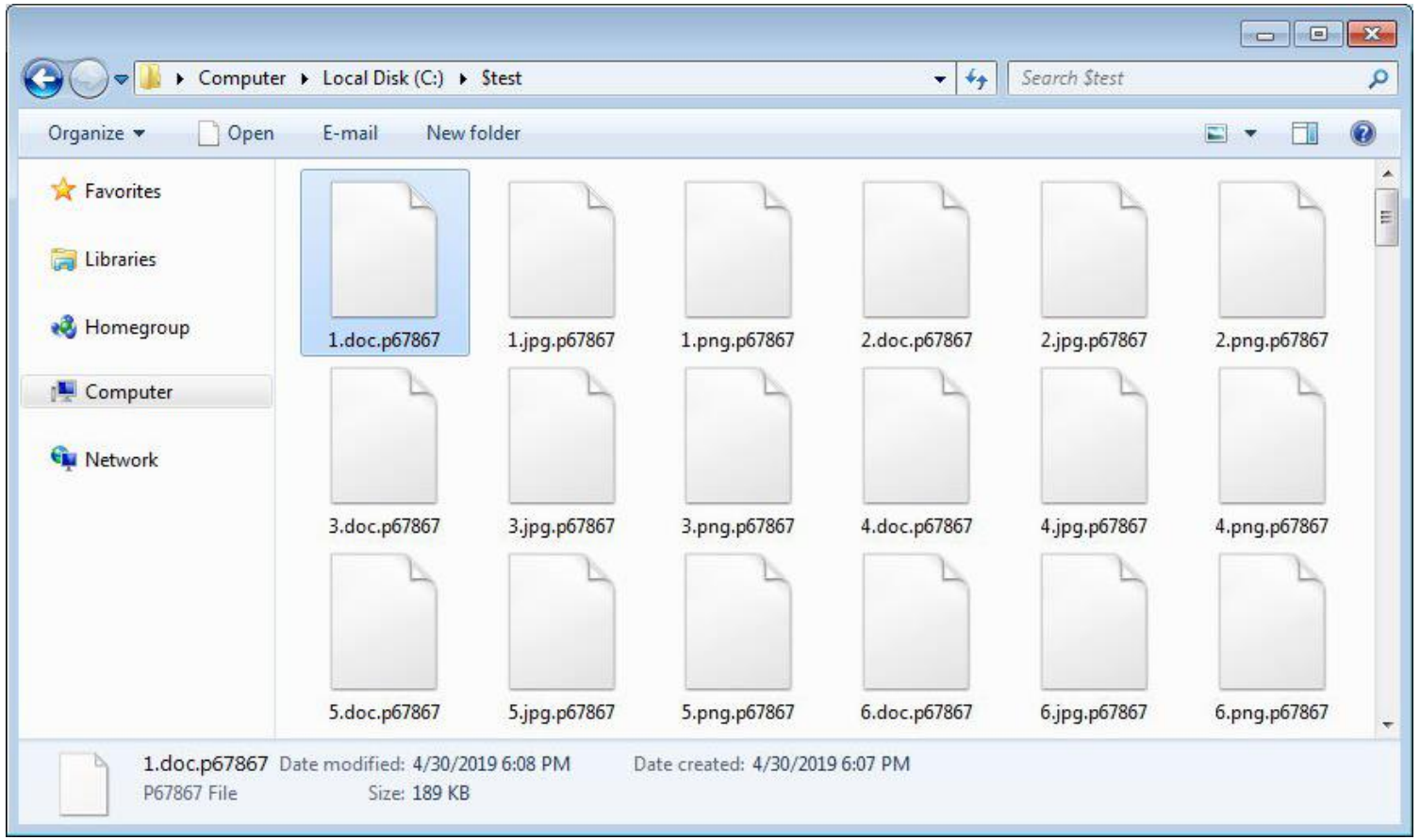
2. One week available to detect intruder before first attempt to exfiltrate data






FLORIDA ORTHOPAEDIC INSTITUTE

# What Ransomware Looks Like To A Practice




**Encrypted Files**

All files on the computer replaced with these encrypted versions instead. These were once DICOM images, now they are garbage

**Jan 2020**
Calm Before the Storm

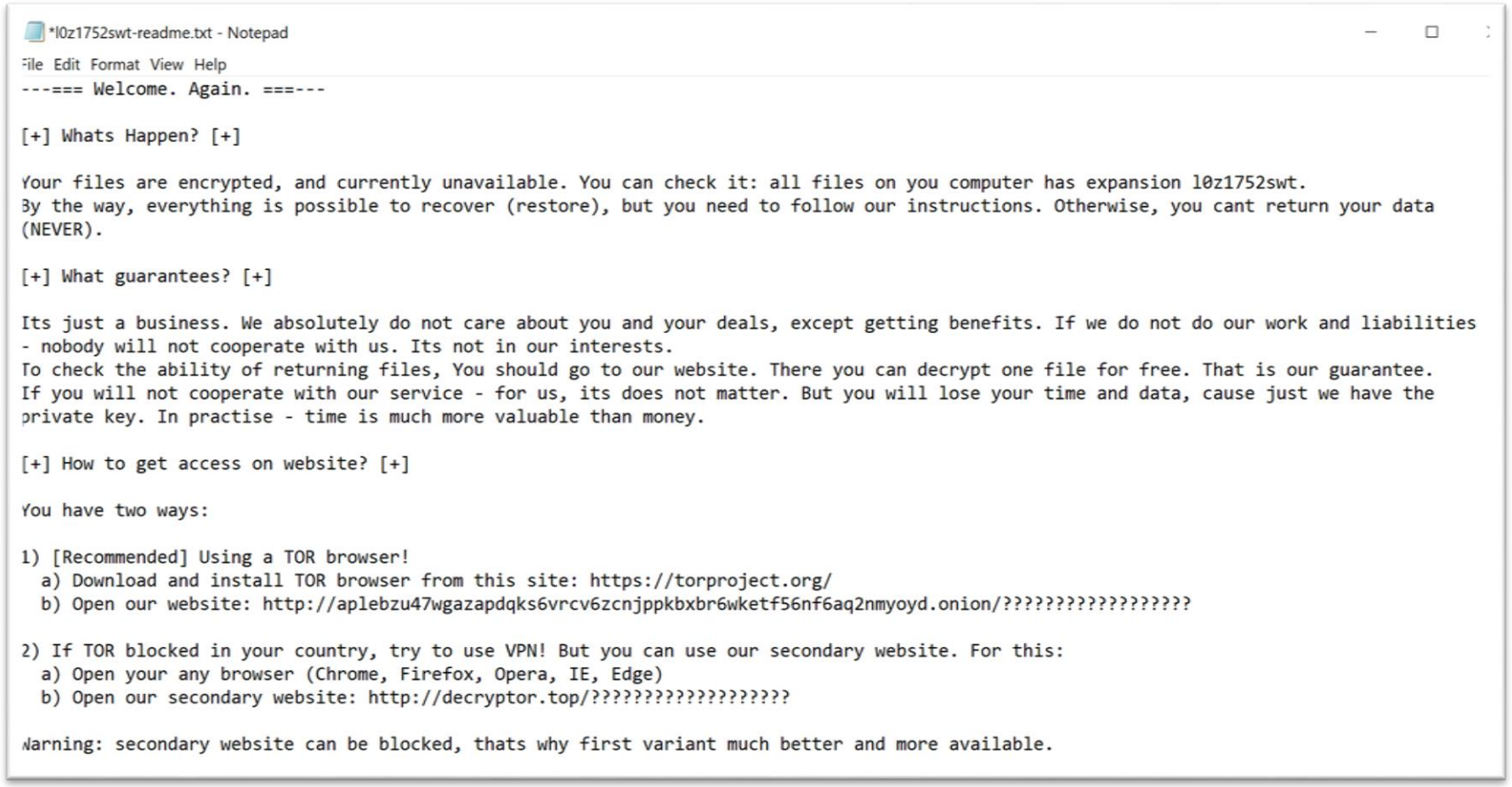
**Mar 2020**
Merger & Covid

**Apr 2020**
Panic



FLORIDA ORTHOPAEDIC INSTITUTE

# What Ransomware Looks Like To A Practice



*l0z1752swt-readme.txt - Notepad

File Edit Format View Help

```
------ Welcome. Again. ======

[+] Whats Happen? [+]

Your files are encrypted, and currently unavailable. You can check it: all files on you computer has expansion l0z1752swt.
By the way, everything is possible to recover (restore), but you need to follow our instructions. Otherwise, you cant return your data
(NEVER).

[+] What guarantees? [+]

Its just a business. We absolutely do not care about you and your deals, except getting benefits. If we do not do our work and liabilities
- nobody will not cooperate with us. Its not in our interests.
To check the ability of returning files, You should go to our website. There you can decrypt one file for free. That is our guarantee.
If you will not cooperate with our service - for us, its does not matter. But you will lose your time and data, cause just we have the
private key. In practise - time is much more valuable than money.

[+] How to get access on website? [+]

You have two ways:

1) [Recommended] Using a TOR browser!
  a) Download and install TOR browser from this site: https://torproject.org/
  b) Open our website: http://aplebzu47wgazapdqks6vrcv6zcnjppkbxbr6wketf56nf6aq2nmyoyd.onion/??????????????????

2) If TOR blocked in your country, try to use VPN! But you can use our secondary website. For this:
  a) Open your any browser (Chrome, Firefox, Opera, IE, Edge)
  b) Open our secondary website: http://decryptor.top/??????????????????

Warning: secondary website can be blocked, thats why first variant much better and more available.
```

**Ransomware Notes**

Getting your files back is easy, just pay a ridiculous amount to someone you can't trust…

surely nothing could go wrong.

**Jan 2020**
Calm Before the Storm

**Mar 2020**
Merger & Covid

**Apr 2020**
Panic



FLORIDA ORTHOPAEDIC INSTITUTE

# Apr 2020 – Initial Recovery

**How do you run an Orthopaedic Practice without computers?**

- Paper Charting
- Viewing Images on the Modality
- No prior studies to review

**What backlog does this create?**

- Scan information back into the EMR
- PACS upload backlog
- Auditing to ensure all documentation is captured

**Lesson's Learned**

1. Disaster Recovery Plan is Key to surviving.
2. Paper may be expensive, but doesn't "go down"
3. Backups take time to restore, plan accordingly




FLORIDA ORTHOPAEDIC INSTITUTE

# Apr 2020 – Call in the Calvary

***How can you get help?***

- Reporting attack to your insurance carrier(s)
  - Cyber Liability Policy
  - Other policies that may provide coverage
- Needed IT Services deployed
- Engaging Counsel
  - Navigating government deadlines
  - Holding insurance carriers accountable
- Informing and obtaining approvals from the Board

**Lesson's Learned**

1. How much coverage do you have?
2. Are there any exclusions or limitations?
3. Who would you want as your counsel?
4. Disaster Recovery Planning




FLORIDA ORTHOPAEDIC INSTITUTE

# June 2020 – Patient Notification

***What does the notification process look like?***

- Required timelines vary (Federal, Each State differs)
- Insurance carrier / attorney response
- Website notification
- Media notification
- Patient Letters
- Third-party services provided to patient

**Lesson's Learned**

1. Staffing for handling phone calls
2. Scripts for physicians and patient facing staff
3. Media response plan




FLORIDA ORTHOPAEDIC INSTITUTE

# July 2020 – Class Action and other after disclosure notables

***What can happen after disclosure?***

**Class Action Lawsuit**

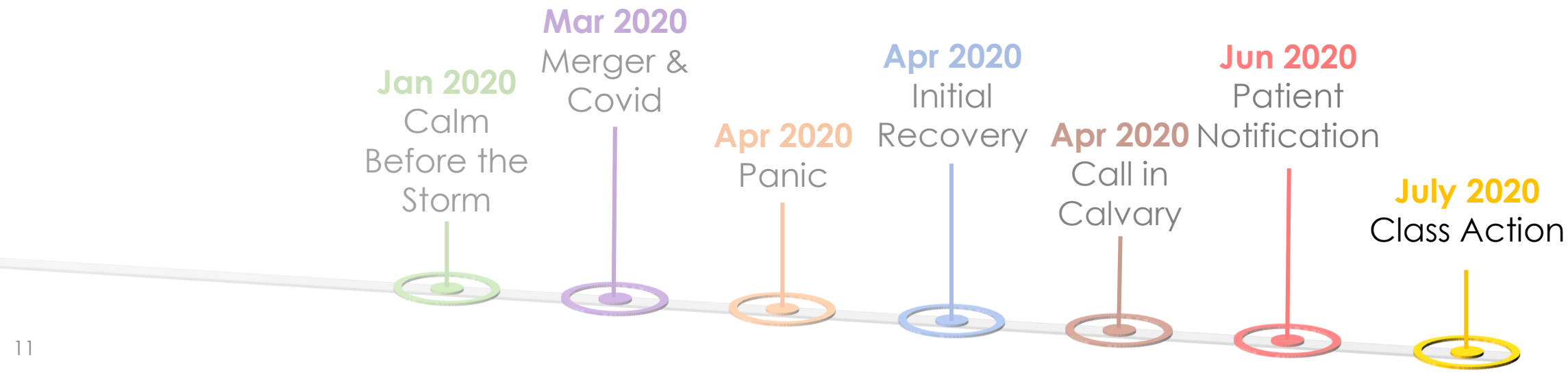
- July 7th - Media announcement - class action lawsuit for $99m
- July 7th - Received copy of actual filing which did not state any specific dollar amount but did confirm suit was filed
- General counsel required approval from carrier July 20th - Preservation of documents issued to key management and board

**Data Loss Concerns**

- External drives linked to company computers experienced data loss spurns an unexpected reaction by one physician

**Lesson's Learned**

1. Prepare your board for the possibilities
2. Understand your insurance policy limitations
3. Disaster recovery planning
4. Clearly define the "*Do Nots*"!






FLORIDA ORTHOPAEDIC INSTITUTE

# Aug 2020 – OCR Questions

***What does the OCR Ask For?***

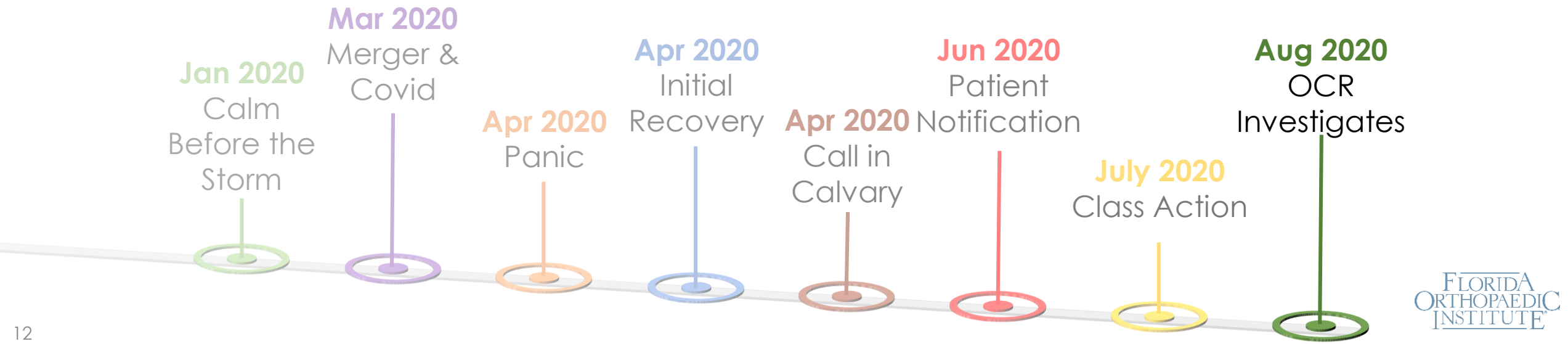
**Everything, Not Just Items Related To This Breach**
- Accounting of Events
- Controls you have in place, why did they fail
- Policies, Procedures, Financials

**Not Just Current, Years of History**
- Combing through past HIPAA gap analysis
- Why didn't you act on a known vulnerability
- What are you doing now, and in the future

**Lesson's Learned**

1. When under an audit, the entire HIPAA guidelines are reviewed.

2. Lawyer integration is key to ensure protection against use by litigation



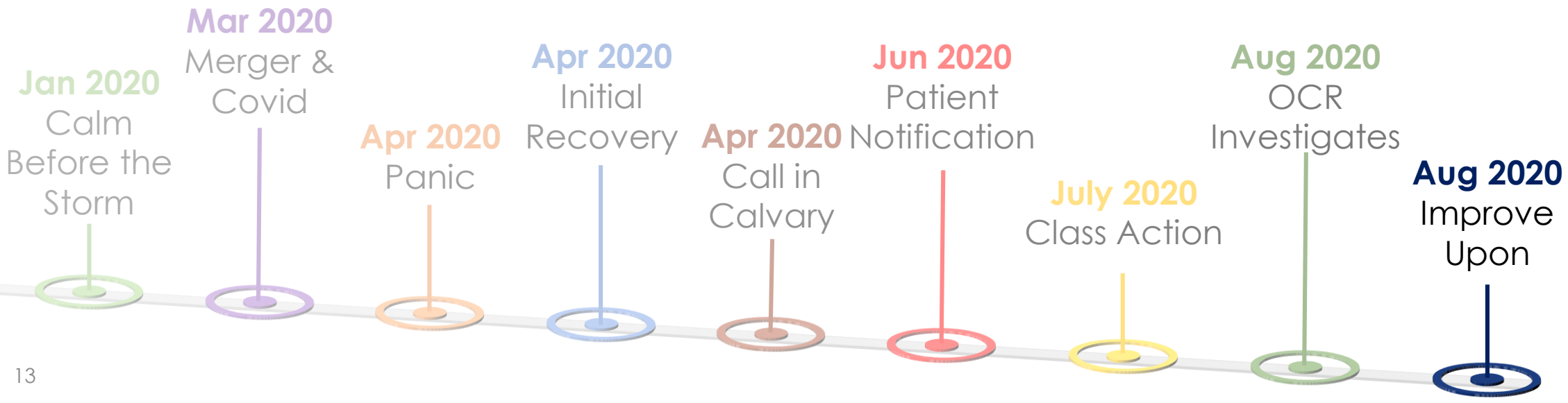
# Aug 2020 – Improve upon

***Have You Documented Your Improvements?***

- ***Technical Improvements***
  - MFA, Logical Separation, Removing Access
  - Data Loss Prevention, Analytics, Logging and Alerting
- ***Administrative Improvements***
  - Policy Rewrites, Inventory, Training, Vendor Assistance
  - Committee Restructure, Budget Expansions
- ***Physical Improvements***
  - Badge Access, Penetration Testing, Getting Rid of Paper

**Lesson's Learned**

1. If you Don't Document it, it didn't happen
2. Looking back is harder than documenting today






FLORIDA ORTHOPAEDIC INSTITUTE

# Current Day

***How long do the ramifications last?***

- Settlement of class action lawsuit completed in February of 2022; however, employee and media notifications did not occur until July 2022. Resulted in additional media attention.
- OCR Investigation ongoing
- As bad as a single breach is, can you recover from multiple breaches?

**Lesson's Learned**

1. Timing of settlement press release
2. Throughout – prepare for questions (creditors/bankers)
3. Focus on documentation!!




FLORIDA ORTHOPAEDIC INSTITUTE

# REFERENCES

## *PPT Co-Authors*

*Ransomware Attacks are Not Humerus; The Insiders View on a Network Compromise and Recovery (2022, October); [PowerPoint Slides]*

- *Florida Orthopaedic Institute*
  - *Janene Culumber, Chief Financial Officer*
  - *Chris Patterson, Director of IT*