A DAM SHAME

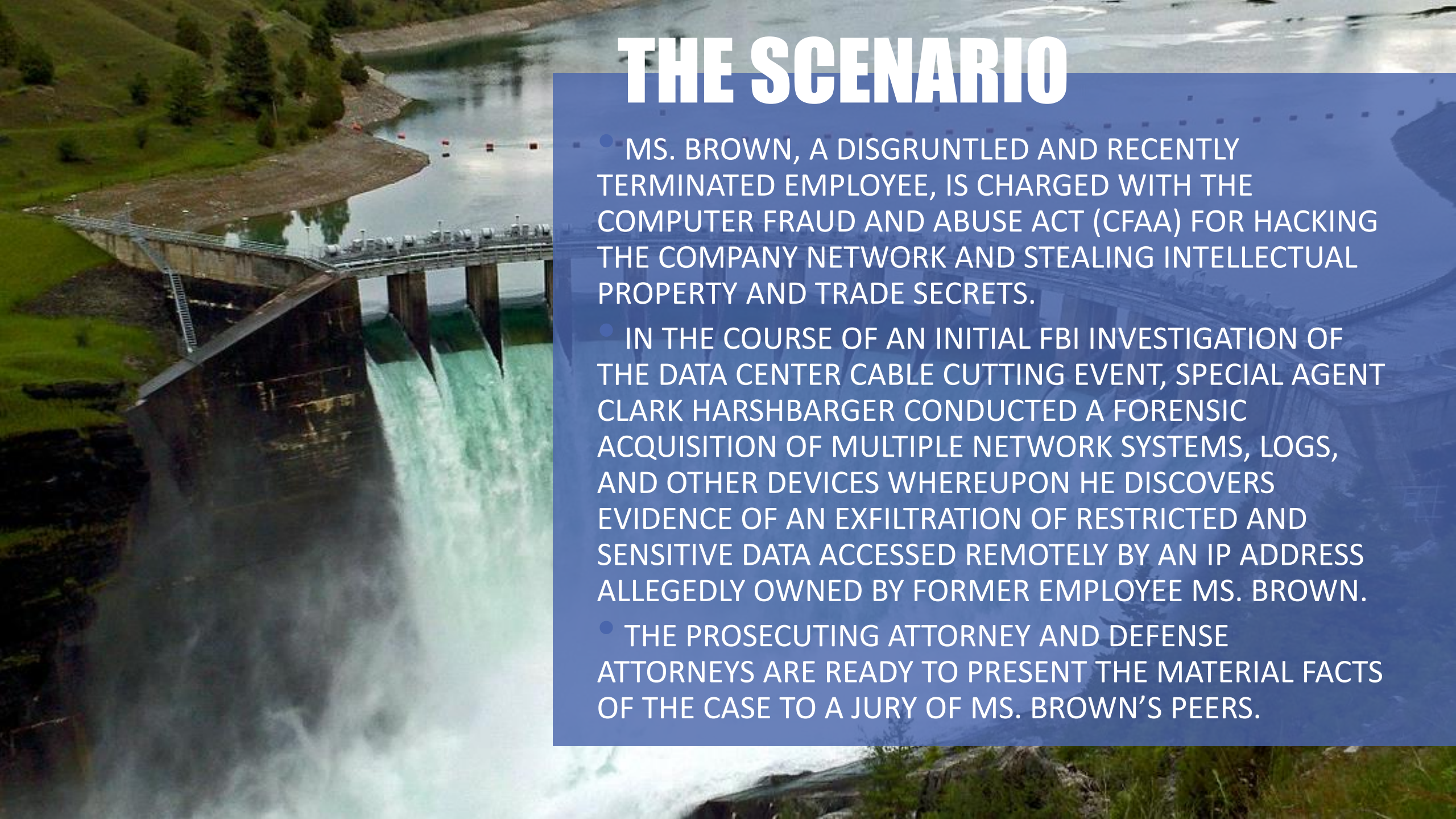
A DATA BREACH MOCK TRIAL

THE RULES

Don’t poke holes in the scenario. Don’t look for technicalities, look for high level issues.

Have fun! This mock trial is intended to be a unique simulation that gives alternative perspectives and future best practice recommendations to participants!

The jury deliberation will commence after the closing statements. Please be respectful and keep an open mind regarding what “reasonable doubt” could potentially mean in this case.



THE SCENARIO

- MS. BROWN, A DISGRUNTLED AND RECENTLY TERMINATED EMPLOYEE, IS CHARGED WITH THE COMPUTER FRAUD AND ABUSE ACT (CFAA) FOR HACKING THE COMPANY NETWORK AND STEALING INTELLECTUAL PROPERTY AND TRADE SECRETS.
- IN THE COURSE OF AN INITIAL FBI INVESTIGATION OF THE DATA CENTER CABLE CUTTING EVENT, SPECIAL AGENT CLARK HARSHBARGER CONDUCTED A FORENSIC ACQUISITION OF MULTIPLE NETWORK SYSTEMS, LOGS, AND OTHER DEVICES WHEREUPON HE DISCOVERS EVIDENCE OF AN EXFILTRATION OF RESTRICTED AND SENSITIVE DATA ACCESSED REMOTELY BY AN IP ADDRESS ALLEGEDLY OWNED BY FORMER EMPLOYEE MS. BROWN.
- THE PROSECUTING ATTORNEY AND DEFENSE ATTORNEYS ARE READY TO PRESENT THE MATERIAL FACTS OF THE CASE TO A JURY OF MS. BROWN’S PEERS.

THE PLAYERS

Judge: Claire Rosston | Holland & Hart LLP | ccrosston@hollandhart.com

Prosecution: Lee Holcomb | Lee Holcomb Consult | lee@leeholcombconsult.com

Defense: Brad Frazer | Hawley Troxell | bfrazer@hawleytroxell.com

Fact Witness: Susan Buxton | DHR | susan.buxton@dhr.Idaho.gov

Fact Witness: Paul Wilch | Hawley Troxell | pwilch@hawleytroxell.com

Expert Witness: Clark Harshbarger | FBI | clark.harshbarger@ic.fbi.gov

Defendant: MacKenzie Brown | Microsoft | macbrown@Microsoft.com

THE PLAYERS

Judge: Claire Rosston | Holland and Hart LLP | ccrosston@hollandhart.com

Prosecution: Lee Holcomb | Lee Holcomb Consult | lee@leeholcombconsult.com

Defense: Brad Frazer | Hawley Troxell | bfrazer@hawleytroxell.com

Expert Witness: Clark Harshbarger | FBI | clark.harshbarger@ic.fbi.gov

Fact Witness: Susan Buxton | DHR | susan.buxton@dhr.Idaho.gov

Fact Witness: Paul Wilch | Hawley Troxell | pwilch@hawleytroxell.com

Defendant: MacKenzie Brown | Microsoft | macbrown@Microsoft.com

COURT IS IN SESSION....

TIMELINE OF EVENTS

Preparation

Ms. Brown Termination

Detection

Cut Cables

Stolen FDA Dam Plans

Containment and Response

FBI Investigation

Remediation

Ms. Brown Arrested

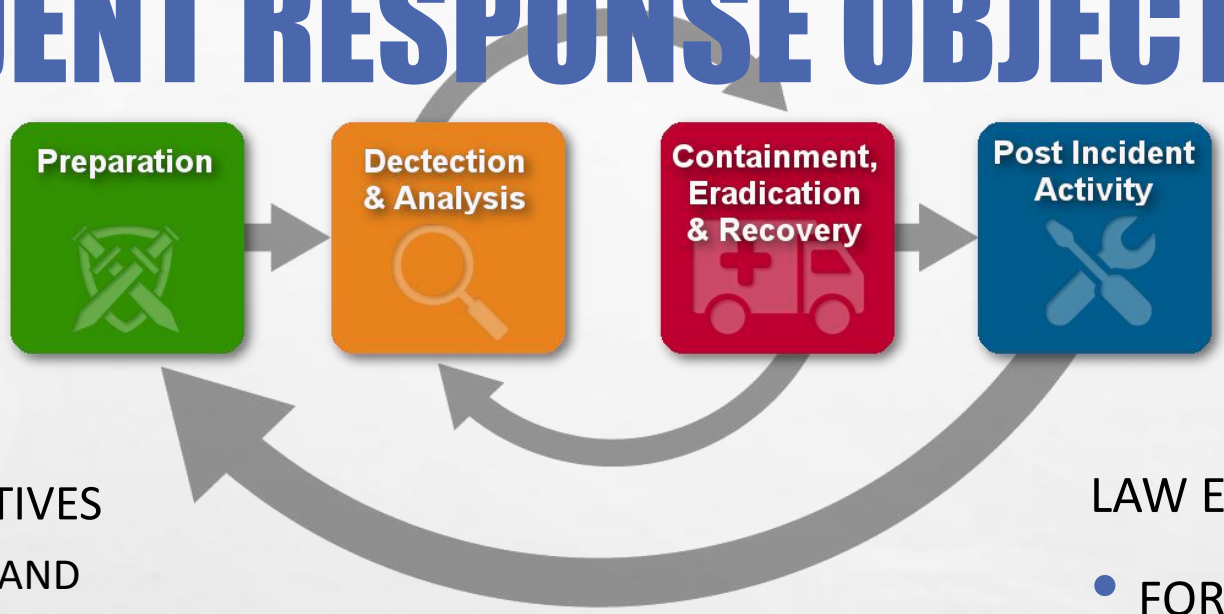
Jail

?

WITNESS 1

SPECIAL AGENT CLARK HARSHBARGER

INCIDENT RESPONSE OBJECTIVES

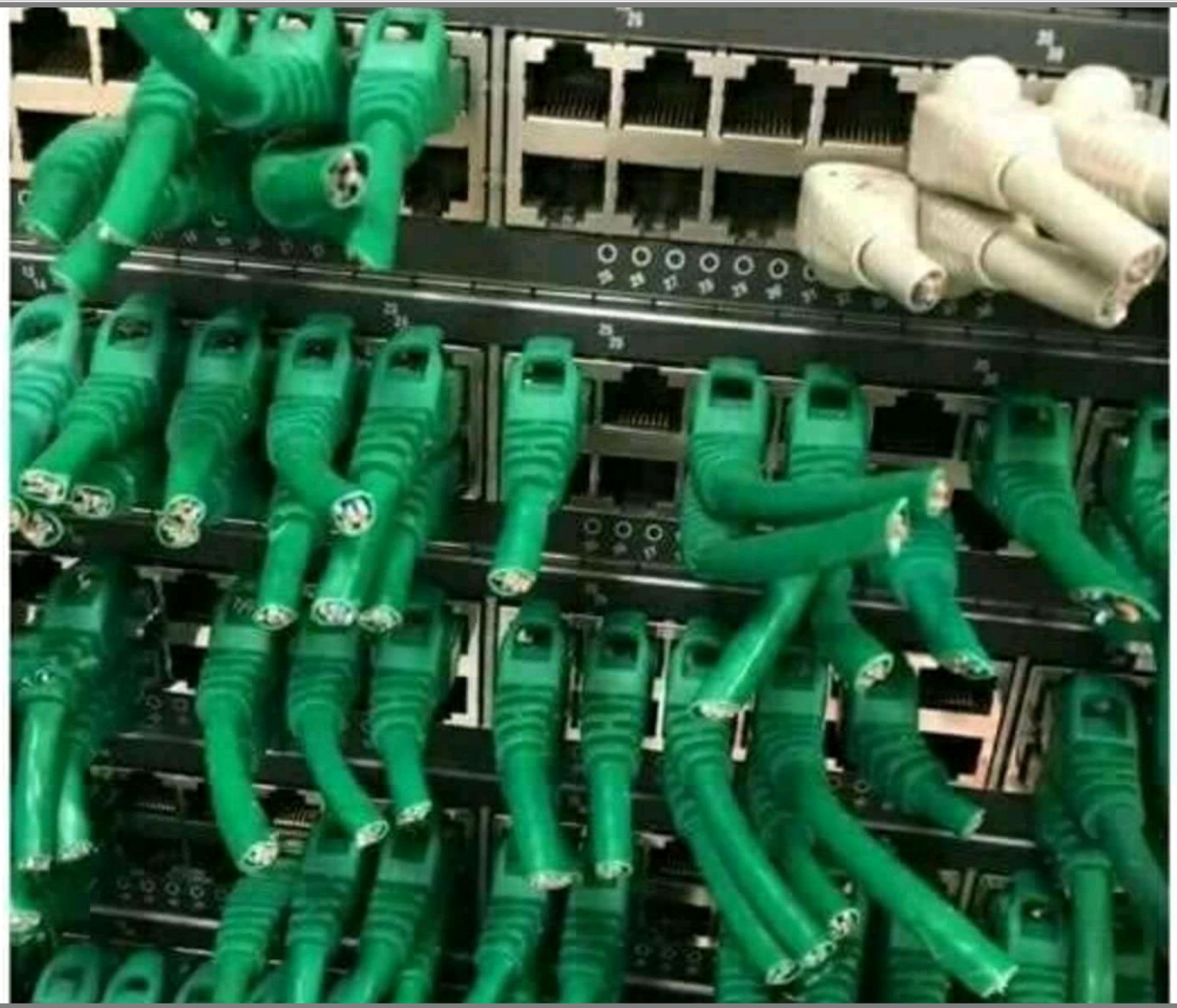


ORGANIZATIONAL OBJECTIVES

- CHAIN OF CUSTODY AND EVIDENCE PRESERVATION
- INCIDENT RESPONSE PLAN AND PROCEDURES
- REPORTING AND NOTIFICATIONS (REGULATORY IF APPLICABLE)
- AFTER ACTION REPORTING

LAW ENFORCEMENT OBJECTIVES

- FORENSICS, ANALYSIS, AND ATTRIBUTION
- TESTIMONY
- REPORTING



INITIAL LAW ENFORCEMENT ENGAGEMENT

EXHIBIT A

CUT CABLES

EXHIBIT B

- EXPRESS VPN
- SUBPOENA

Express VPN, LLC
Attn: Custodian of Records
13 Jersey Ave
Princeton, NJ 07001
Fax (609) 238-6330
Voice (609) 238-5318

In re: Subscriber information for referenced IP access:

Express VPN Server 13.33.151.156 access of 24.119.187.122 on or after April 15, 2018 21:52 UST.

For the period of April 15, 2018 to present, records for the subscriber information as listed above, and any other associated accounts, to include, but not limited to:

(A) Subscriber information and Billing records

(B) Connection records, or records of session times and durations, including local and long distance
telephone connection numbers and information;

(C) Telephone or instrument number or other subscriber number or identity, including any temporarily
assigned network addresses;

(D) Means, source, and history of payments for such service (including any credit card or bank
account numbers);

(E) MAC addresses associated with connection records; and

(F) Monthly usage history of uploads and downloads for corresponding MAC address history.

If possible, please provide this information in a standardized electronic format. If electronic format is unavailable, then a readable hard-copy will suffice.

You may comply with this subpoena by providing this information directly to the Special Agent named on the cover letter of this document.

EXHIBIT C

- CABLE ONE
- SUBPOENA

Cable One, Inc
Attn: Custodian of Records
2550 Boise Ave
Boise, ID 83702
Fax (208) 868-6330
Voice (208) 868-5318

In re: Subscriber information provided:

For the period of April 15, 2018 to present, records for the subscriber information as listed above, and
any other associated accounts, to include, but not limited to:

(A) Subscriber Information

(B) Type of Service (Cable modem, DSL, dial-up, etc) and Length of service (including start date) and types of service utilized;

(C) Connection records, or records of session times and durations, including local and long-distance telephone connection numbers and information;

(D) Telephone or instrument number or other subscriber number or identity, including any temporarily assigned network addresses;

(E) Means, source, and history of payments for such service (including any credit card or bank account numbers);

(F) MAC addresses associated with connection records; and

(G) Monthly usage history of uploads and downloads for corresponding MAC address history.

If possible, please provide this information in a standardized electronic format. If electronic format is unavailable, then a readable hard-copy will suffice.

You may comply with this subpoena by providing this information directly to the Special Agent named on the cover letter of this document.

- D-14 02:27:10 13.33.151.156 %ASA-4-152018: Built inbound TCP connection 2495301911 for outside:VPN (VPN)(LOCAL/000420171) to inside:JLCCDB (CUSTDB)
-
- D-10 02:27:10 24.119.188.104 %ASA-4-152018: Built outbound UDP connection 2495301911 for outside:JLCCDB (CUSTDB)(LOCAL/000420171) to inside:WEBPORTAL/53 (WEBPORTAL/53)
-
- D-7 02:27:10 13.33.151.156 %ASA-4-152018: Built outbound TCP connection 2495301911 for outside:WEBPORTAL/55135 (WEBPORTAL/55135)(LOCAL/000420171) to inside:66.171.248.178/443 (66.171.248.178/443)

- 24.119.187.122 JLCC Static IP—FDA Database Outside Access
-
- 13.33.151.156 Express VPN Accessed April 18, 2019 through April 19, 2019 from 24.119.188.104

- 24.119.188.104 Mac Brown Home from April 16, 2019 through April 19, 2019

EXHIBIT D

FDA OWNED DEVICE FROM DEFENDANT'S RESIDENCE

WITNESS 2

PAUL WILCH

KEY STATE LAWS: BREACH NOTIFICATION

Covers	Requirements	Enforcement	Liability	Federal breach notification
• All states and DC have a breach notification law • Which state's law applies depends on where the impacted person residence by the governor	• Trigger: Discovery or notification of breach • Deadline: Varies	• Typically AG - Some states authorize civil suits by injured individuals	• Injunction • Economic damages • Regulator costs • Fines	• HIPAA breach notification rule • FCC privacy regulations

EXHIBIT D

FDA OWNED DEVICE FROM DEFENDANT'S RESIDENCE

WITNESS 3

SUSAN BUXTON

BEST PRACTICES WITH THIRD-PARTY SERVICE PROVIDERS

Have a written contract with the provider

- It's not just a best practice; it's the law:
  - Federal enforcement FTC Act § 5
  - Industry regulations in the financial and health care sectors
  - State laws (e.g., CA and MA)

that contains contract terms that require:

- Proper physical, administrative and technical safeguards
  - Employee training
  - Written NDA with employees who receive customer's confidential information
- Compliance with applicable data security and privacy laws
- Indemnification
- Cyberinsurance

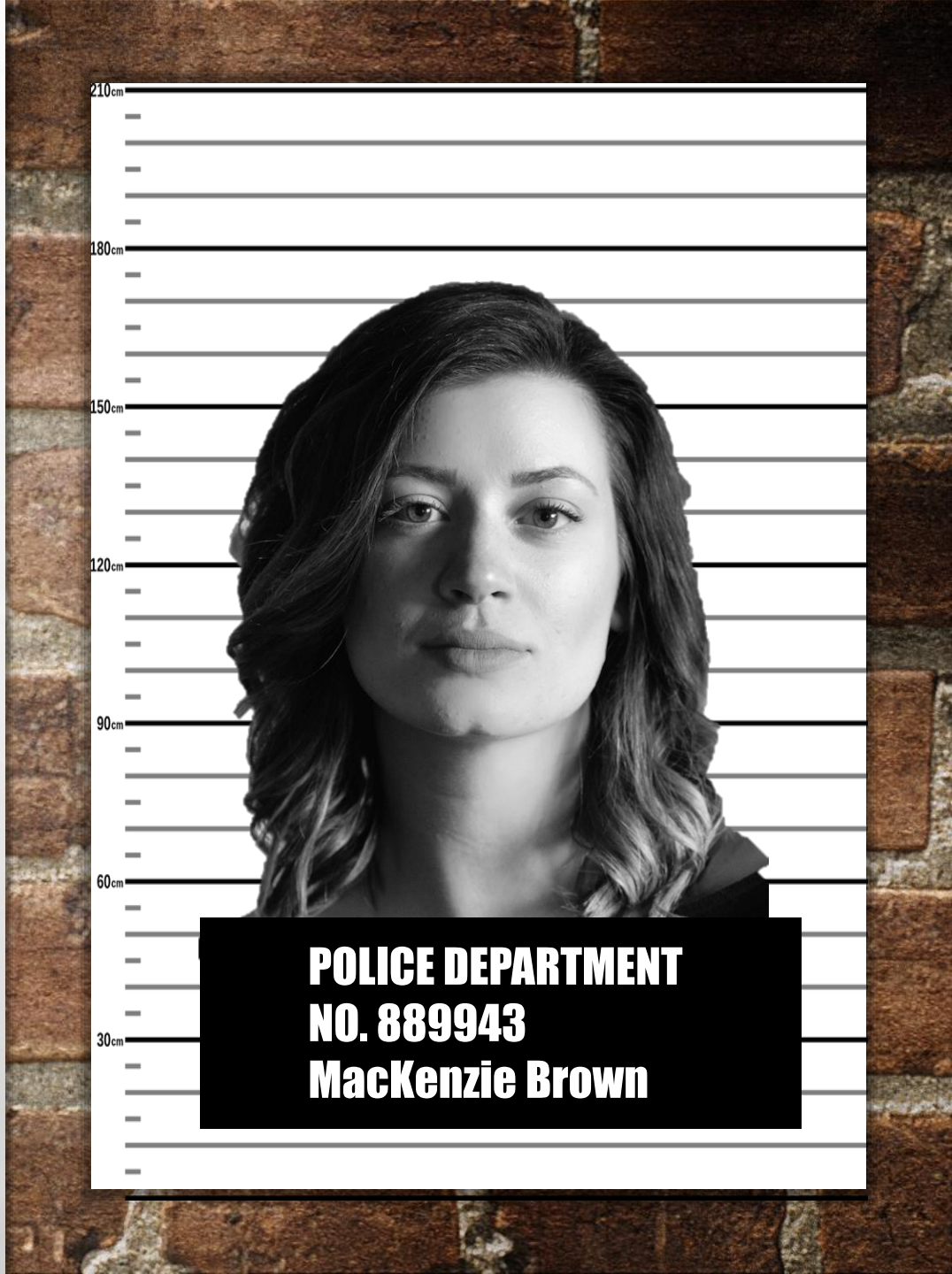
INSIDER THREAT CONSIDERATIONS

PROCESSES AND RESOURCES

- POLICIES, PLANS, SOP'S
- EMPLOYEE HANDBOOK
- NON-DISCLOSURE AGREEMENT
- ACCEPTABLE USE POLICY
- BACKGROUND CHECKS
- THIRD-PARTY RISK MANAGEMENT
- TERMINATION PROTOCOLS
- INCIDENT RESPONSE PLAN & PLAYBOOKS (RUNBOOK FOR CLASSIFIED INSIDER THREAT INCIDENT)
- BYOD POLICY (MOBILE DEVICE MANAGEMENT, INVENTORY)
- INSIDER THREAT PROGRAM (BEHAVIOR AND ACCOUNT ANOMALIES AND ALERTS)

THE ACCUSED

MACKENZIE BROWN



THE JURY IS OUT

FINAL DELIBERATION

TAKEAWAYS

1. WRITTEN CYBERINCIDENT RESPONSE PLAN: KNOW WHOM TO CALL.
2. FORENSICALLY SECURE ALL EVIDENCE AND DATA OF THE HACK.
3. WRITTEN CYBERSECURITY POLICIES AND PROCEDURES.
4. CYBERLIABILITY INSURANCE OR SELF-INSURANCE.
5. LOGGING ALL NETWORK ACCESS.
6. PRINCIPLE OF LEAST PRIVILEGE: LIMIT ACCESS TO DATA TO “NEED TO KNOW”.
7. CONTRACTUAL OBLIGATIONS OF SERVICE PROVIDERS/CLOUD VENDORS.
8. EMPLOYEE TRAINING AND SIGNED POLICY MANUALS.
9. CERTIFICATIONS FOR SECURITY PERSONNEL.
10. EMPLOYEE EXIT PROCEDURES.
11. NOTIFICATION OBLIGATIONS TO INSURER TO INVOKE COVERAGE.
12. DATA BREACH REPORTING OBLIGATIONS FOR PII.