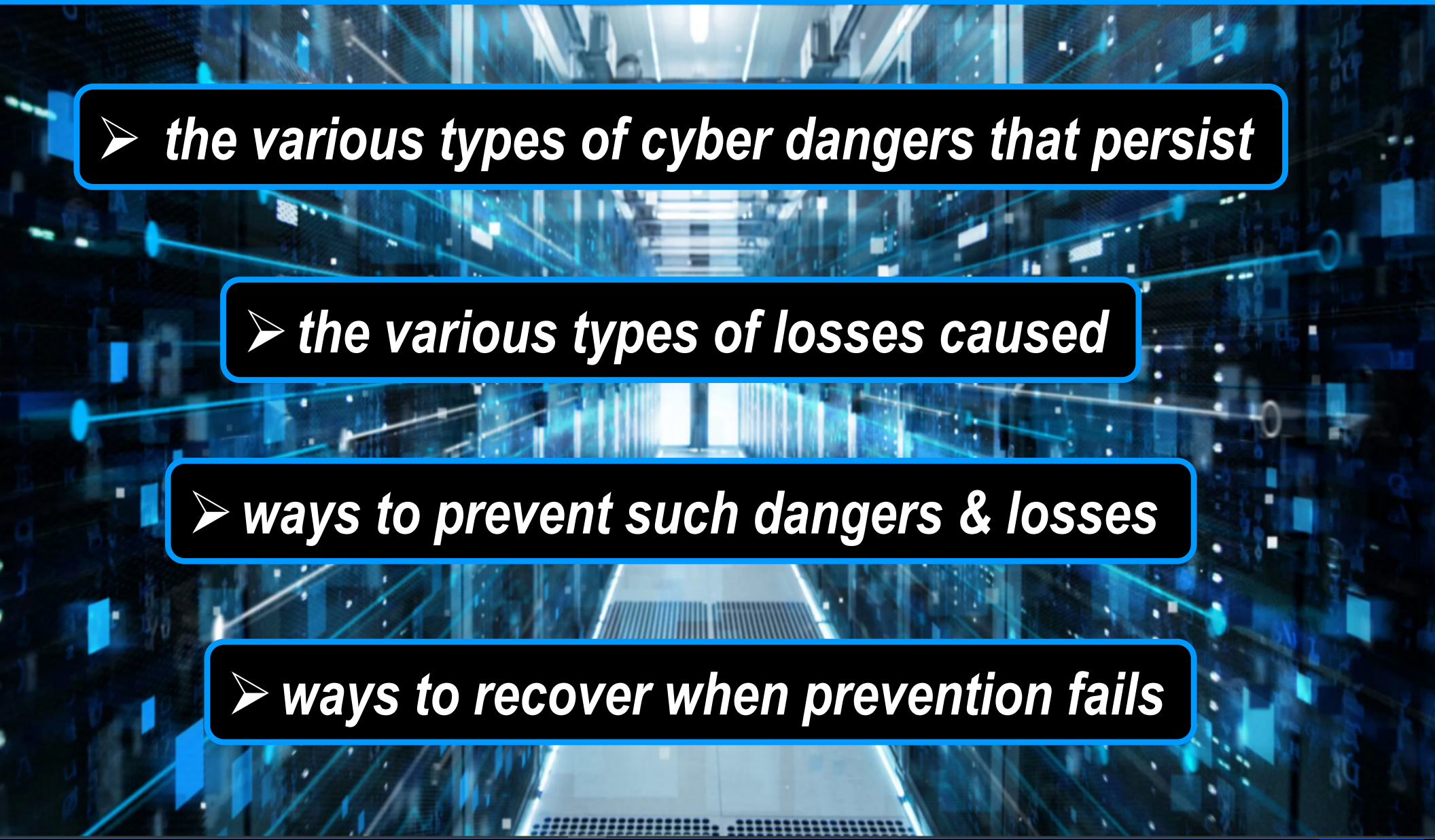
WASHINGTON PUBLIC PORTS ASSOCIATION

3:15 – 4:05 PM

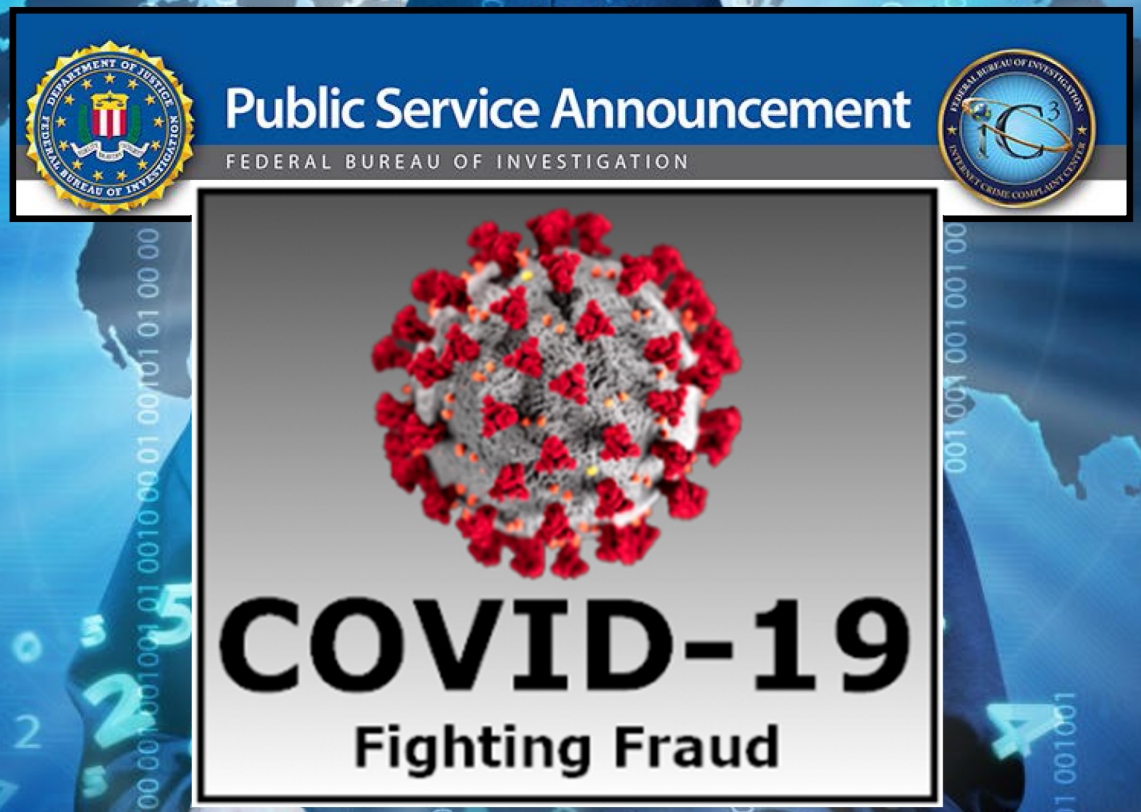
- CYBER THREATS AND INTRUSIONS
- WHAT TO DO IN CASE OF AN INTRUSION
- RELATED INSURANCE ISSUES
- ETC.

CYBERCRIME DANGERS FOR PORTS



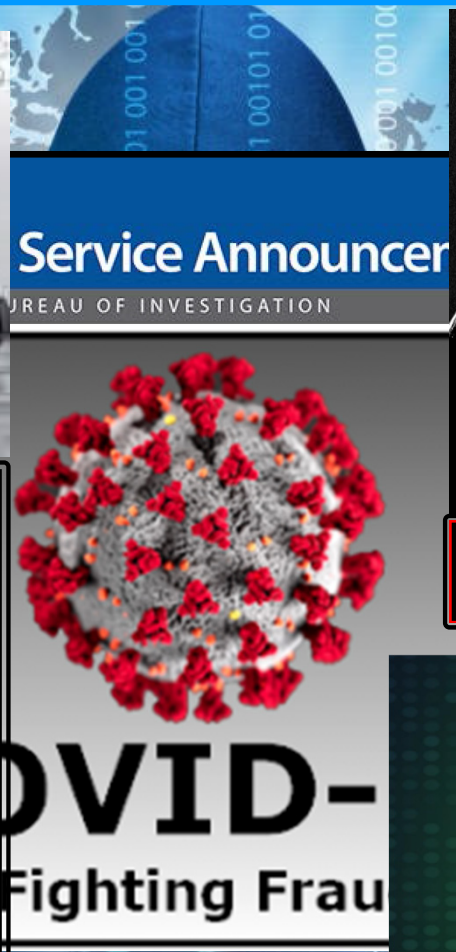
- the various types of cyber dangers that persist
- the various types of losses caused
- ways to prevent such dangers & losses
- ways to recover when prevention fails

Climate Changes That Have Increased Cybercrime



Climate Changes That Have Increased Cybercrime

Ukraine Humanitarian Crisis



Russian Cyberattacks

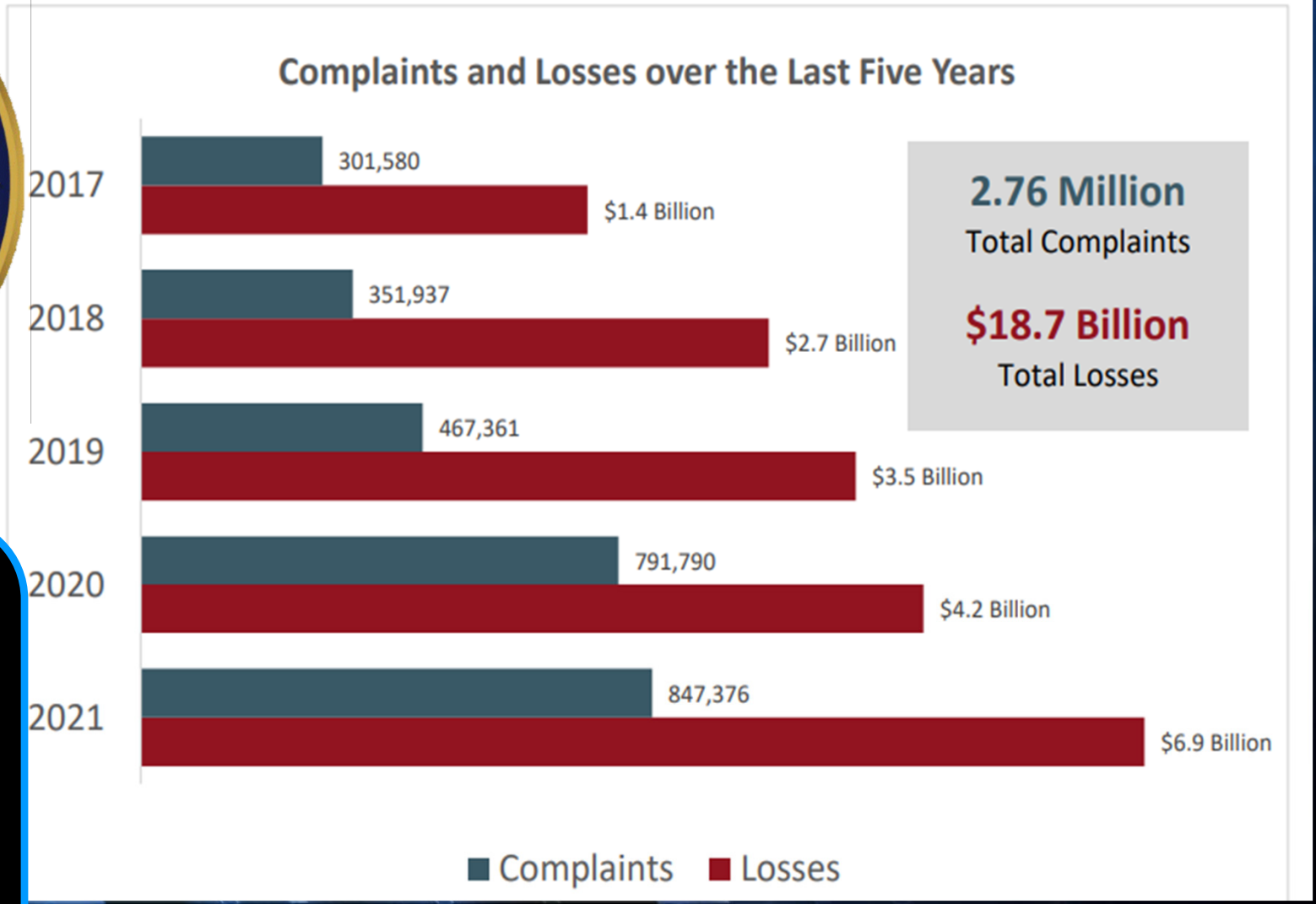
North Korea, China, Iran Cyberactivity

Foster Garvey
Tom Ahearne
ahearne@foster.com / 206-295-8868

12/6/2022
Cyber issues CLE

WASHINGTON PORTS

CYBERCRIME'S CONTINUED GROWTH



...with our State in the top-ten for most cybercrime

- ***victims*** *and*
- ***dollars lost***

Broad Types Of Cyber Dangers That Persist

Broad Types Of Cyber Dangers That Persist

Phishing/Vishing/Smishing/Pharming: The use of unsolicited email, text messages, and telephone calls purportedly from a legitimate company requesting personal, financial, and/or login credentials.

Spoofing: Contact information (phone number, email, and website) is deliberately falsified to mislead and appear to be from a legitimate source. For example, spoofed phone numbers making mass robo-calls; spoofed emails sending mass spam; forged websites used to mislead and gather personal information. Often used in connection with other crime types.

Tech Support: Subject posing as technical or customer support/service.

Business Email Compromise/Email Account Compromise: BEC is a scam targeting businesses (not individuals) working with foreign suppliers and/or businesses regularly performing wire transfer payments. EAC is a similar scam which targets individuals. These sophisticated scams are carried out by fraudsters compromising email accounts through social engineering or computer intrusion techniques to conduct unauthorized transfer of funds.

Broad Types Of Cyber Dangers That Persist

Malware/Scareware/Virus: Software or code intended to damage, disable, or capable of copying itself onto a computer and/or computer systems to have a detrimental effect or destroy data.

Ransomware: A type of malicious software designed to block access to a computer system until money is paid.

Denial of Service/TDoS: A Denial of Service (DoS) attack floods a network/system, or a Telephony Denial of Service (TDoS) floods a voice service with multiple requests, slowing down or interrupting service.

Corporate Data Breach: A data breach within a corporation or business where sensitive, protected, or confidential data is copied, transmitted, viewed, stolen, or used by an individual unauthorized to do so.

The Various Types Of Losses Caused

- Loss of information

- Loss of computer systems

- Loss of money

Loss of Information

Loss of Information

Business information

(contracts, financial data, internal emails, accounts, etc.)

Employee information

(W-2 information, drivers license/state ID number, SSN, name/date of birth, direct deposit account number, health information, reviews, etc.)

Security & vulnerability information

(security & response plans, security cameras/systems, lines/pipes/details, maintenance/repair/shift/shipping schedules, etc.)

Contractor/vender information

(contacts, responsibilities, overlaps, gaps, accounts, etc.)

Simplified example: ***Premera Blue Cross Customer Data Security Breach Litigation***, 2019 WL 3410382 (D.Ore. 2019)

- Case involved data breach into Premera's computer server.
- To prevent data breaches, Premera gave employees security training on avoiding malicious social engineering tactics, phishing emails, and telephone call spoofing.
- Hacker created a domain name similar to Premera's domain name ("@premrera.com" rather than "@premera.com").
- Using that similar domain, hacker sent a Premera employee an email purporting to be from Premera IT with a link to download a document. Employee clicked on the link, which downloaded malware giving the hacker access to Premera's server.
- That gave hacker access to confidential information of Premera members & employees on the server.
- Class action suit against Premera on behalf of persons whose confidential information had been taken.
- Discovery disclosed that Premera's IT security team had repeatedly complained they were understaffed, with one member, for example, stating he felt like he was on a "sinking ship" trying to protect the server from data breaches.

➢ **Court:** approved settlement that required Premera to
(1) pay $32 million into a plaintiff settlement fund ***and***
(2) pay $42 million on improved data security by 2022

Loss of Computer Systems

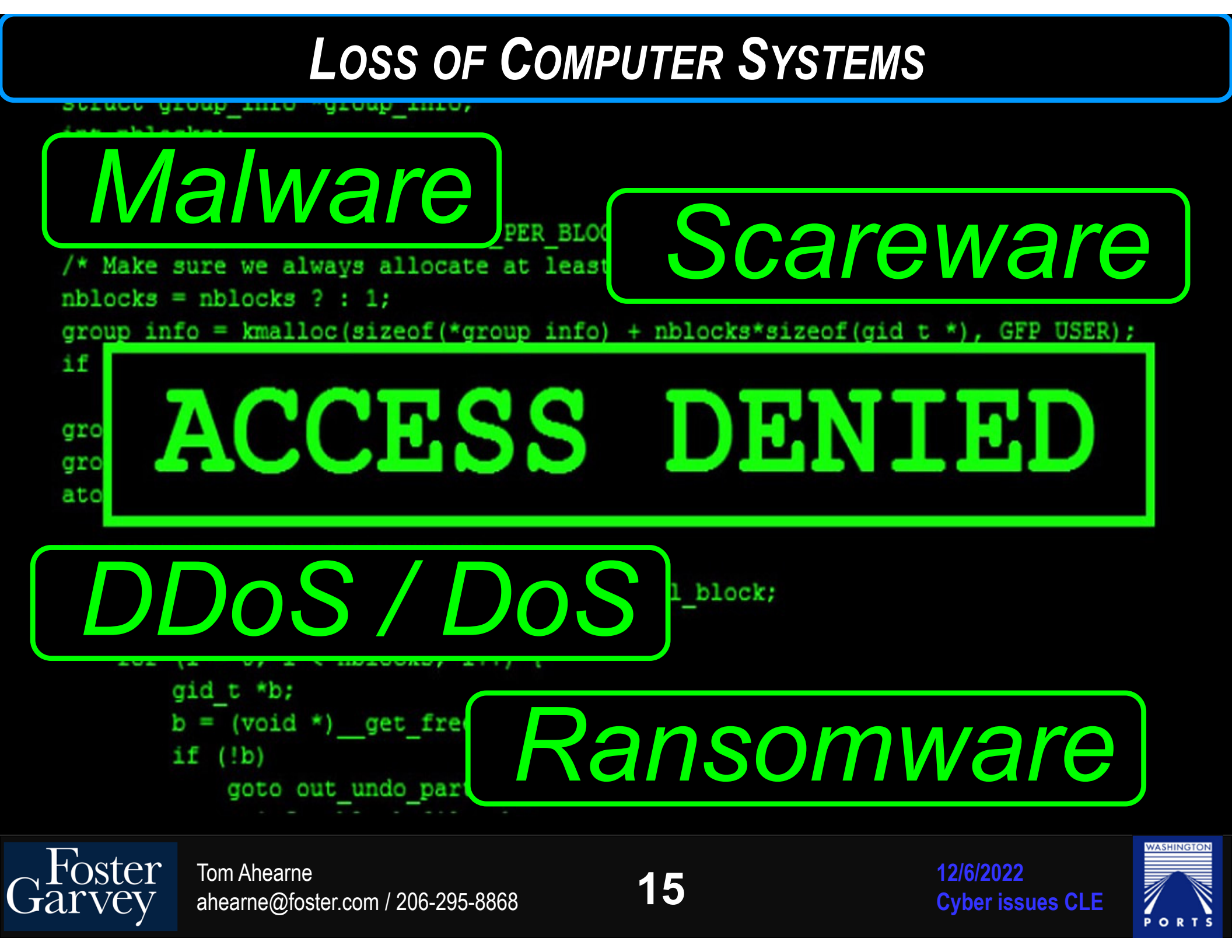
```
int nblocks;
int i;

nblocks = (gidsetsize + NGROUPS_PER_BLOCK - 1) / NGROUPS_PER_BLOCK;
/* Make sure we always allocate at least one indirect block pointer */
nblocks = nblocks ? : 1;
group_info = kmalloc(sizeof(*group_info) + nblocks*sizeof(gid_t *), GFP_USER);
if
gro
gro
ato

if (gidsetsize <= NGROUPS_SMALL)
    group_info->blocks[0] = group_info->small_block;
else {
    for (i = 0; i < nblocks; i++) {
        gid_t *b;
        b = (void *)__get_free_page(GFP_USER);
        if (!b)
            goto out_undo_partial_alloc;
```

ACCESS DENIED

Loss of Computer Systems



LOSS OF COMPUTER SYSTEMS

Ransomware examples

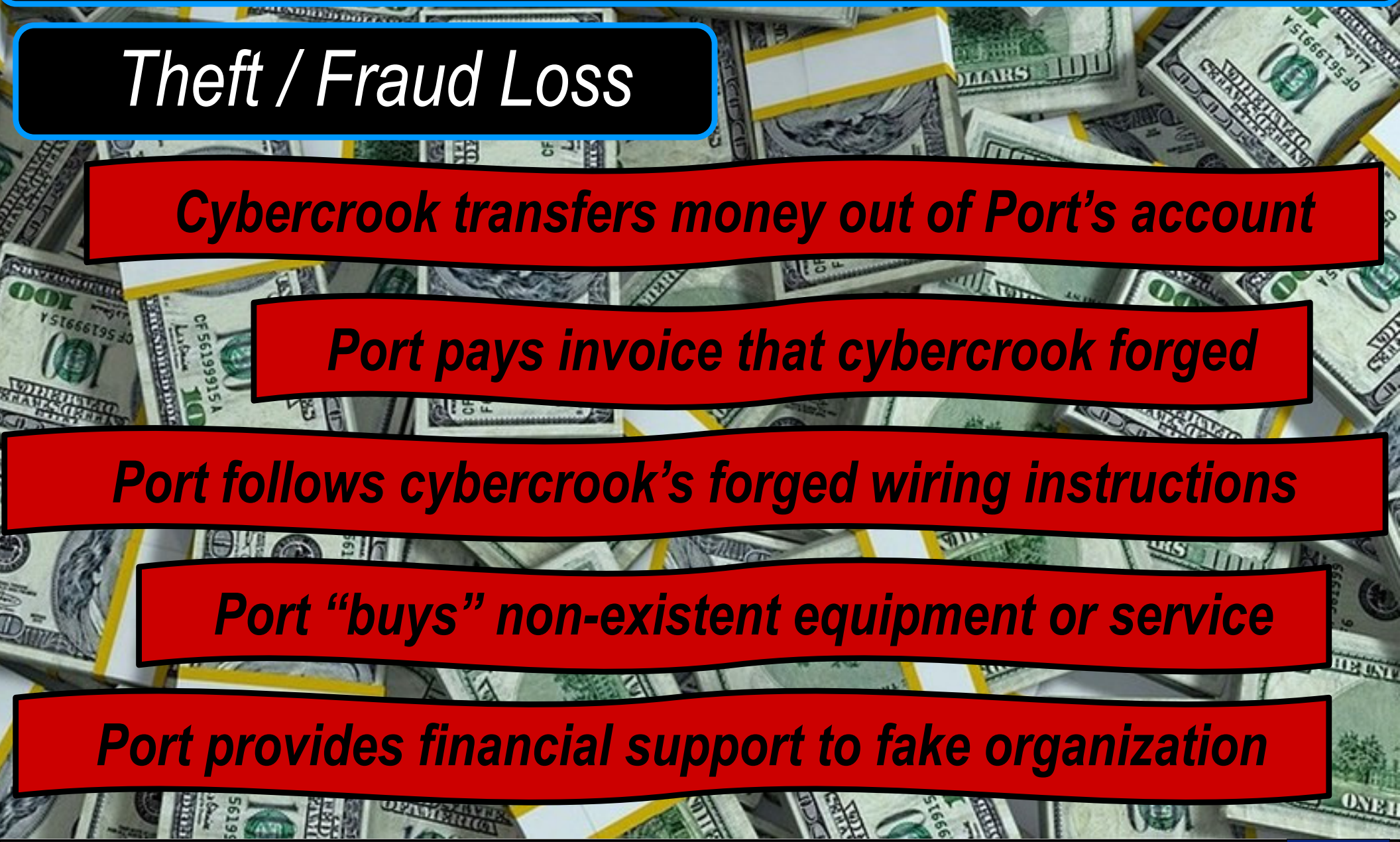
- Sometimes relatively small & (with fingers crossed) paid:
  - ***$10K*** paid by Leominster district (MA)
  - ***$10K*** paid by Horry County system (SC)
  - ***$460K*** paid by Lake City (FL)
  - ***$600K*** paid by City of Riviera Beach (FL)
- Other times the ransom is not paid (which is FBI's advice) – but costs victim millions to restore its computer system:
  - ***$18 million*** to restore Baltimore's computer system after refusing to pay $75K ransom
  - ***$17 million*** to restore Atlanta's computer system after refusing to pay $51K ransom

Ransomware

Loss of Money

Loss of Money

Theft / Fraud Loss



Cybercrook transfers money out of Port's account

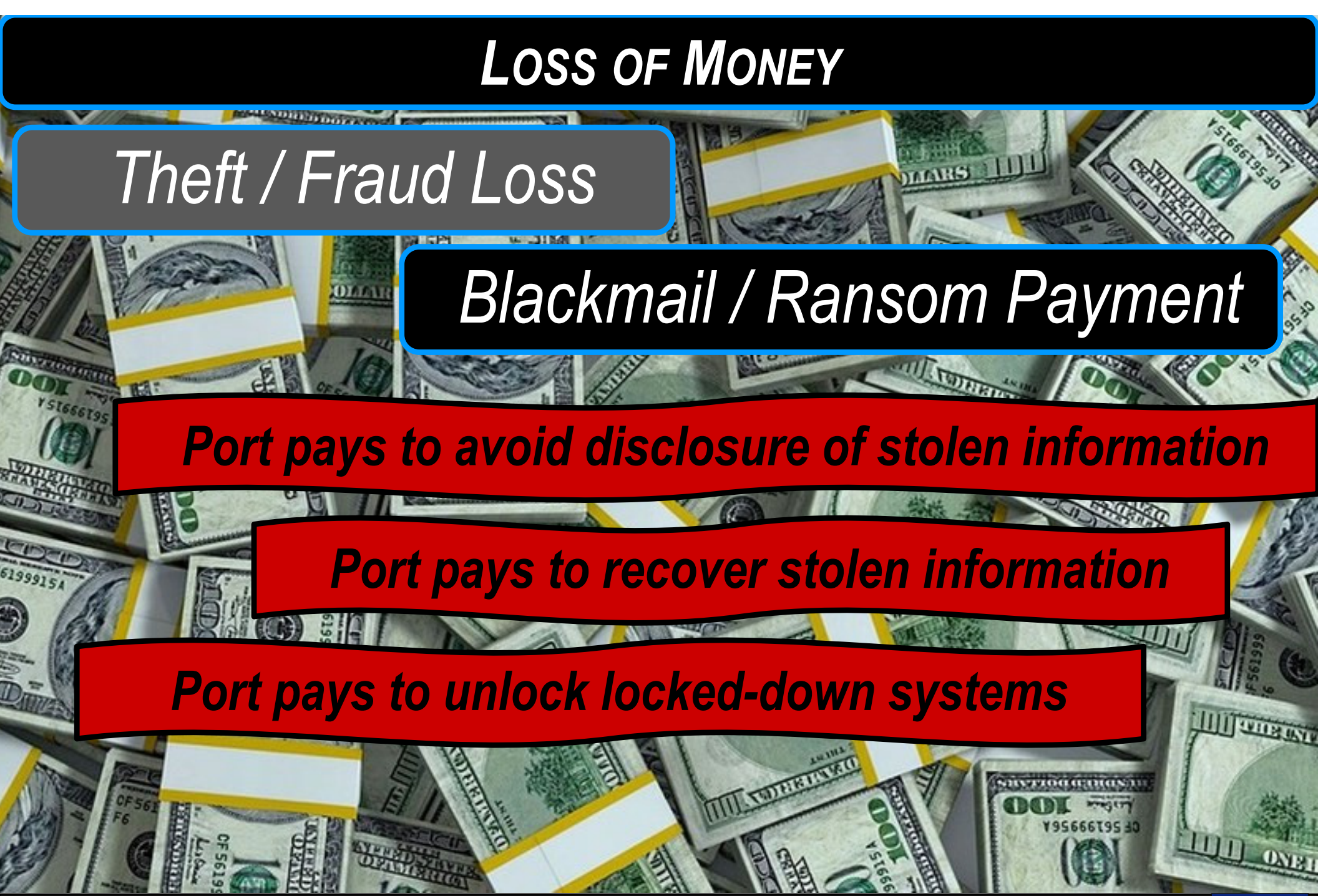
Port pays invoice that cybercrook forged

Port follows cybercrook's forged wiring instructions

Port "buys" non-existent equipment or service

Port provides financial support to fake organization

Loss of Money



Theft / Fraud Loss

Blackmail / Ransom Payment

Port pays to avoid disclosure of stolen information

Port pays to recover stolen information

Port pays to unlock locked-down systems

Loss of Money

Theft / Fraud Loss

Blackmail / Ransom Payment

Investigation & Response Costs

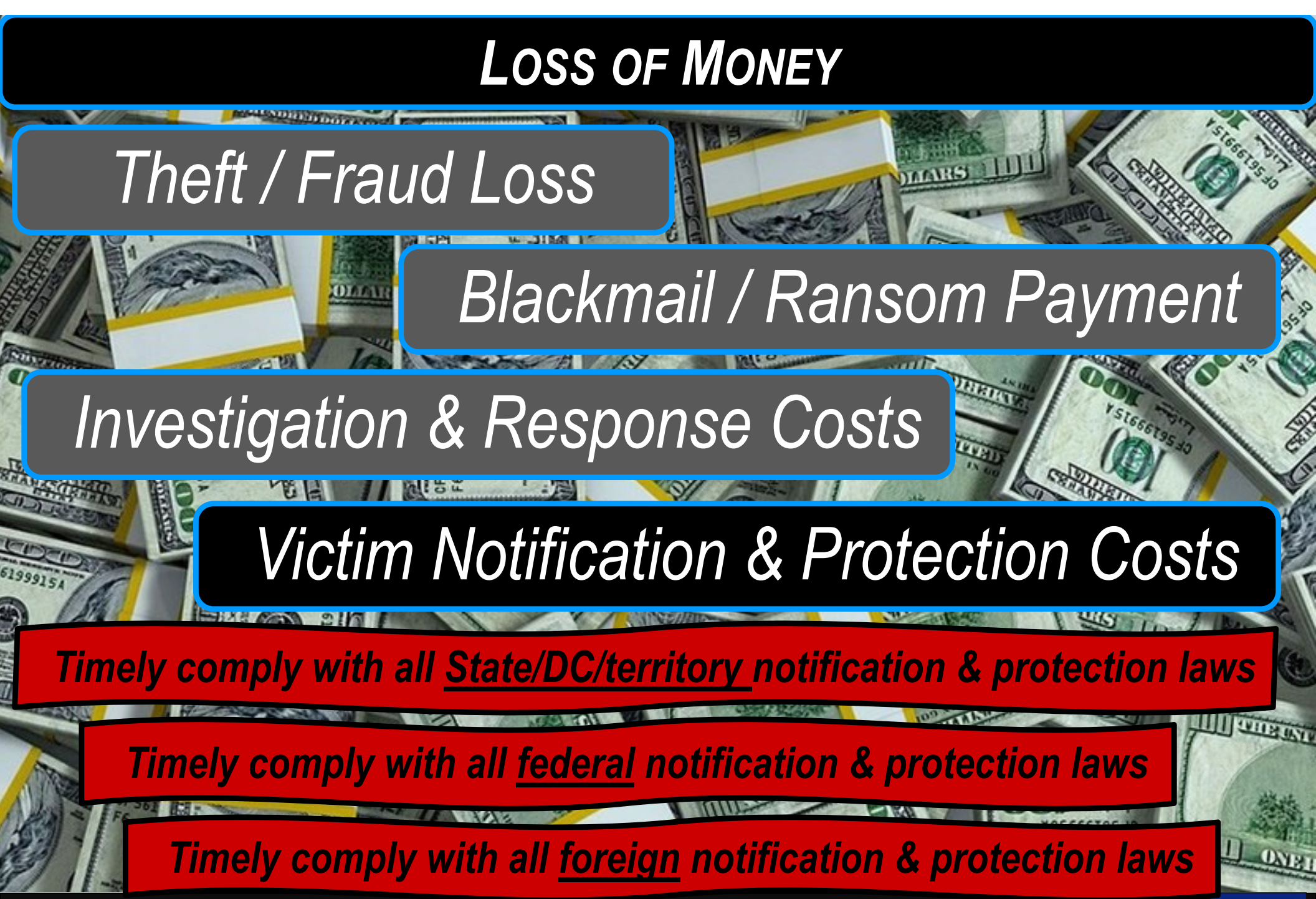
Promptly determining cause & timing of the breach

Immediate lock-down of system to stop further damage

Promptly determining the full extent/scope of the breach

Promptly determining all legal obligations triggered

Loss of Money



Theft / Fraud Loss

Blackmail / Ransom Payment

Investigation & Response Costs

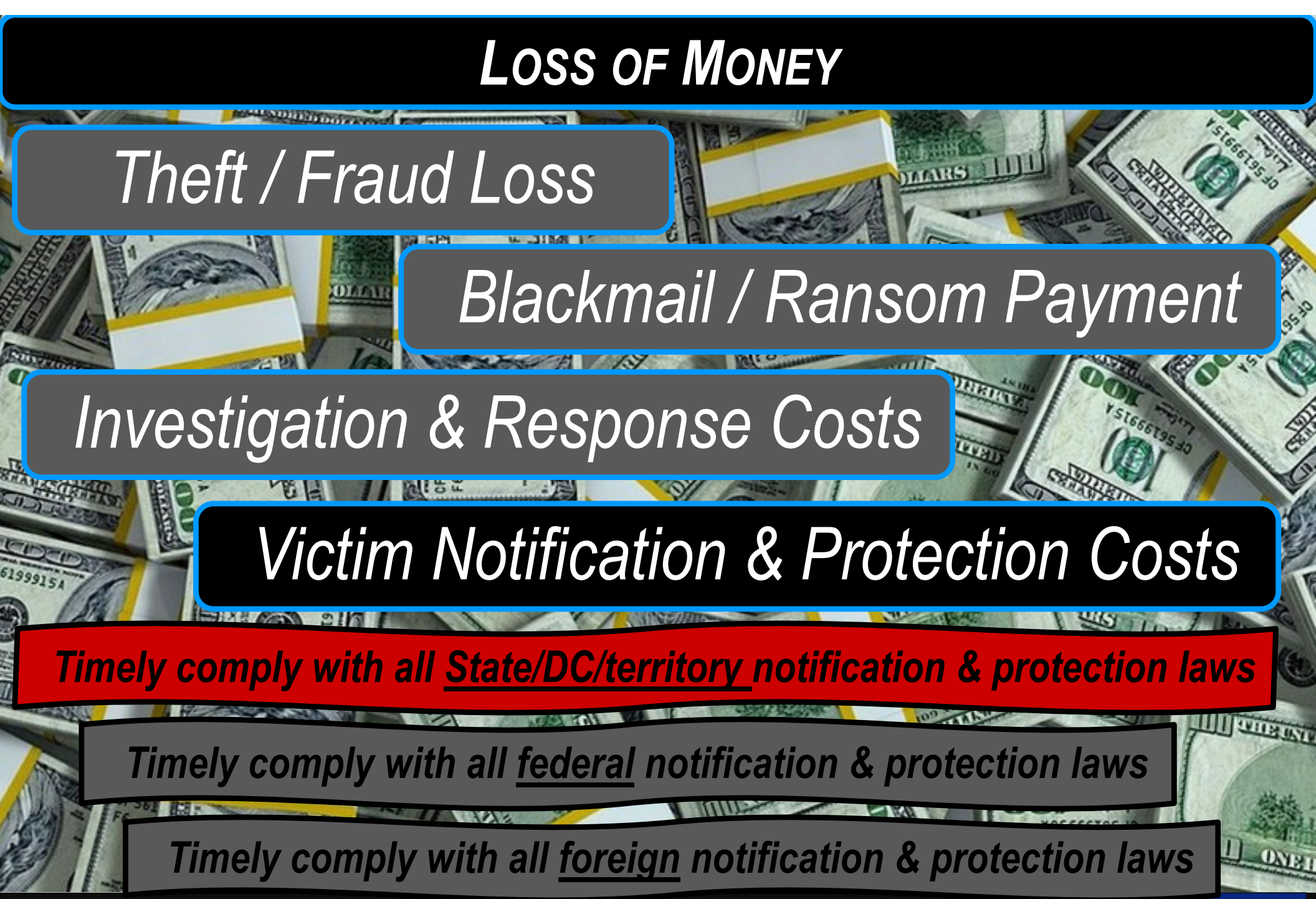
Victim Notification & Protection Costs

Timely comply with all State/DC/territory notification & protection laws

Timely comply with all federal notification & protection laws

Timely comply with all foreign notification & protection laws

Loss of Money



Theft / Fraud Loss

Blackmail / Ransom Payment

Investigation & Response Costs

Victim Notification & Protection Costs

Timely comply with all State/DC/territory notification & protection laws

Timely comply with all federal notification & protection laws

Timely comply with all foreign notification & protection laws

Released Information Triggers

WA : name plus one of following: DOB, SSN, driver lic #, state/student/military ID #, health info, med ins info, credit card # with password, acct # with password, etc., etc., etc. *[RCW 19.255.005 & 42.56.590]*

Montana: list also included taxpayer ID # *[MCA 30-14-1704]*

Victim Protection Requirements

WA: written notice, including toll-free telephone numbers & addresses of the major credit reporting agencies *[RCW 19.255.010 & 42.56.590]*

CA: written notice, including 12 months of free identity theft protection & mitigation services *[Cal. Civ. Code 1798.82(d)(2)(G)]*

Victim Notice Deadline

WA : "the most expedient time possible, without unreasonable delay, and no more than 30 calendar days after the breach was discovered" *[RCW 19.255.010 & 42.56.590]*

Puerto Rico: within 10 days of breach discovery *[10 L.P.R.A. §4052]*

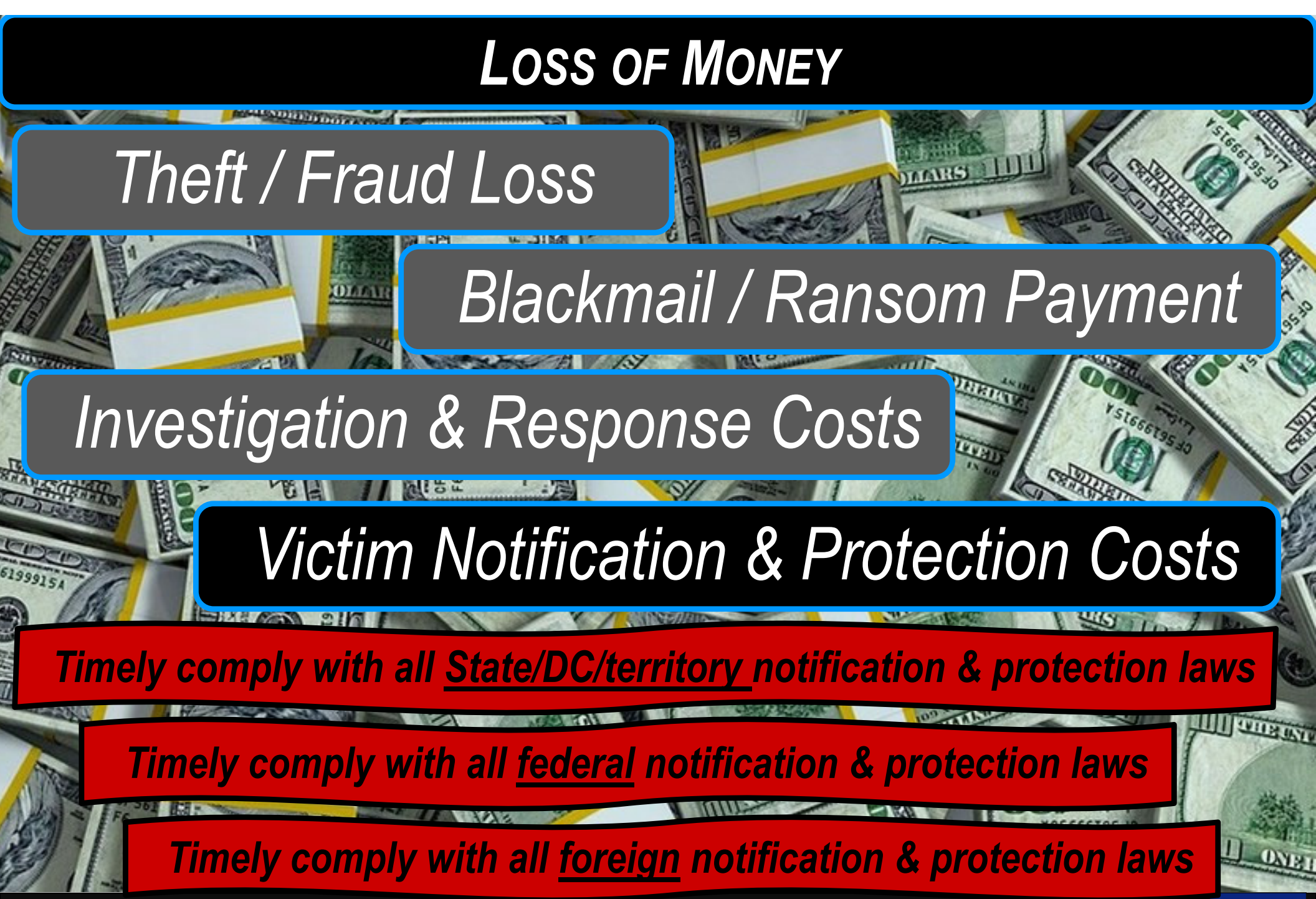
Timely comply with all State/DC/territory notification & protection laws

Attorney General Submission Trigger

WA : 500 WA residents *[RCW 19.255.010 & 42.56.590]*

NV: no trigger since no AG submission required

Loss of Money



Theft / Fraud Loss

Blackmail / Ransom Payment

Investigation & Response Costs

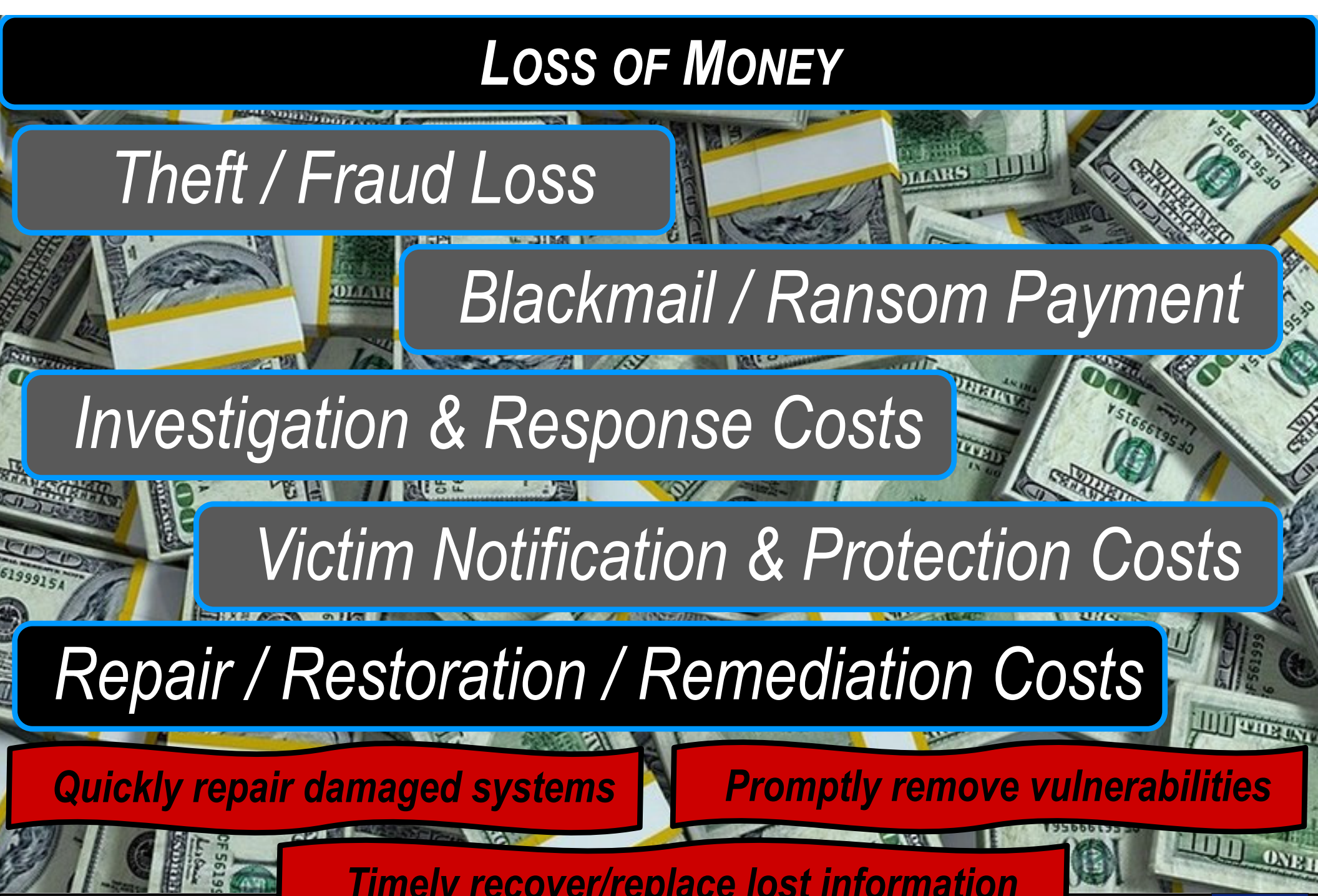
Victim Notification & Protection Costs

Timely comply with all State/DC/territory notification & protection laws

Timely comply with all federal notification & protection laws

Timely comply with all foreign notification & protection laws

Loss of Money



Theft / Fraud Loss

Blackmail / Ransom Payment

Investigation & Response Costs

Victim Notification & Protection Costs

Repair / Restoration / Remediation Costs

Quickly repair damaged systems

Promptly remove vulnerabilities

Timely recover/replace lost information

Loss of Money

- Theft / Fraud Loss
- Blackmail / Ransom Payment
- Investigation & Response Costs
- Victim Notification & Protection Costs
- Repair / Restoration / Remediation Costs
- Lawsuits & Judgments

Loss of Money

Theft / Fraud Loss

Port pays lawyers, experts, etc. defending claims/lawsuits by plaintiffs whose information was disclosed in the breach

Port pays settlements/judgments resulting from such claims/lawsuits

Port pays lawyers, experts, etc. defending claims/lawsuits by vendors/contractors not paid since cybercrook was paid instead

Port pays settlements/judgments resulting from such claims/lawsuits

Port pays lawyers, experts, etc. pursuing claims/lawsuits against others fully or partially liable for the loss

Lawsuits & Judgments

Ways To Prevent Such Dangers & Losses

Ways To Prevent Such Dangers & Losses

- Require ongoing & productive security training
- Conduct ongoing vulnerability & weakness testing
- Periodically search for sleeper cells/programs/moles
- Limit access to those who need access
- Impose up-to-date authentication protocols
- Eliminate shortcut features that play into cybercrook tactics
- Let no Trojan horse in *(flash drives, tapped links, opening attachments, old devices)*
- Keep virus protections up to date
- Maintain a thorough & universally understood emergency response plan

Ways To Recover When Prevention Fails

- Law enforcement

- Insurance

- Litigation

IMMEDIATELY CONTACT FBI, LAW ENFORCEMENT, & BANKS

IMMEDIATELY CONTACT FBI, LAW ENFORCEMENT, & BANKS

Immediately report suspected cyberfraud to FBI:
FBI's Internet Crime Complaint Center (www.ic3.gov).

Further document with reports to the FBI at https://www.ic3.gov/default.aspx, BEC.IC3.gov., local FBI field office, and National Center for Disaster Fraud Hotline at disaster@leo.gov.

Hack the Hackers
- find a key to take the money back

Bank Holds
- freeze funds before they leave the country
- seize funds in the country

Criminal Charges
- Wire Fraud
- Computer Intrusion
- Identity Theft
- Money Laundering

IMMEDIATELY CONTACT FBI, LAW ENFORCEMENT, & BANKS

<u>Immediately</u> contact local police
(*contacting police to generate a police report could also be a coverage requirement under your insurance).*

<u>Immediately</u> contact your financial institution:
demand a recall of funds – push hard & fast. *(need to stop U.S. banking system's transfer before your money leaves the country.)*

Promptly Pursue Insurance Claims

PROMPTLY PURSUE INSURANCE CLAIMS

1. get a <u>complete</u> copy of <u>all</u> <u>potentially</u> applicable insurance policies

2. read & understand each policy's fine print:

- ➔ **know how to phrase your claim**
  (e.g, under your policy's "theft of money" coverage or "employee failure to faithfully perform duties" coverage – which could make the difference between policy limits of, for example, $50K as opposed to $1 million)
- ➔ **know how fast must you give the insurance company notice**
  (e.g., "as soon as possible" after discovery?)
- ➔ **know what information you must give the insurance company**
  (e.g., how & when loss occurred? Books & records?)
- ➔ **know what reporting to police is required**
  (e.g., must notify police to generate a police report?)

IMMEDIATELY PREPARE FOR POTENTIAL LITIGATION

[as defendant as well as plaintiff]

IMMEDIATELY PREPARE FOR POTENTIAL LITIGATION

[as defendant as well as plaintiff]

Prepare to defend claims/lawsuits by plaintiffs whose information was disclosed in the breach

Prepare to defend claims/lawsuits by venders/contractors not paid since cybercrook was paid instead

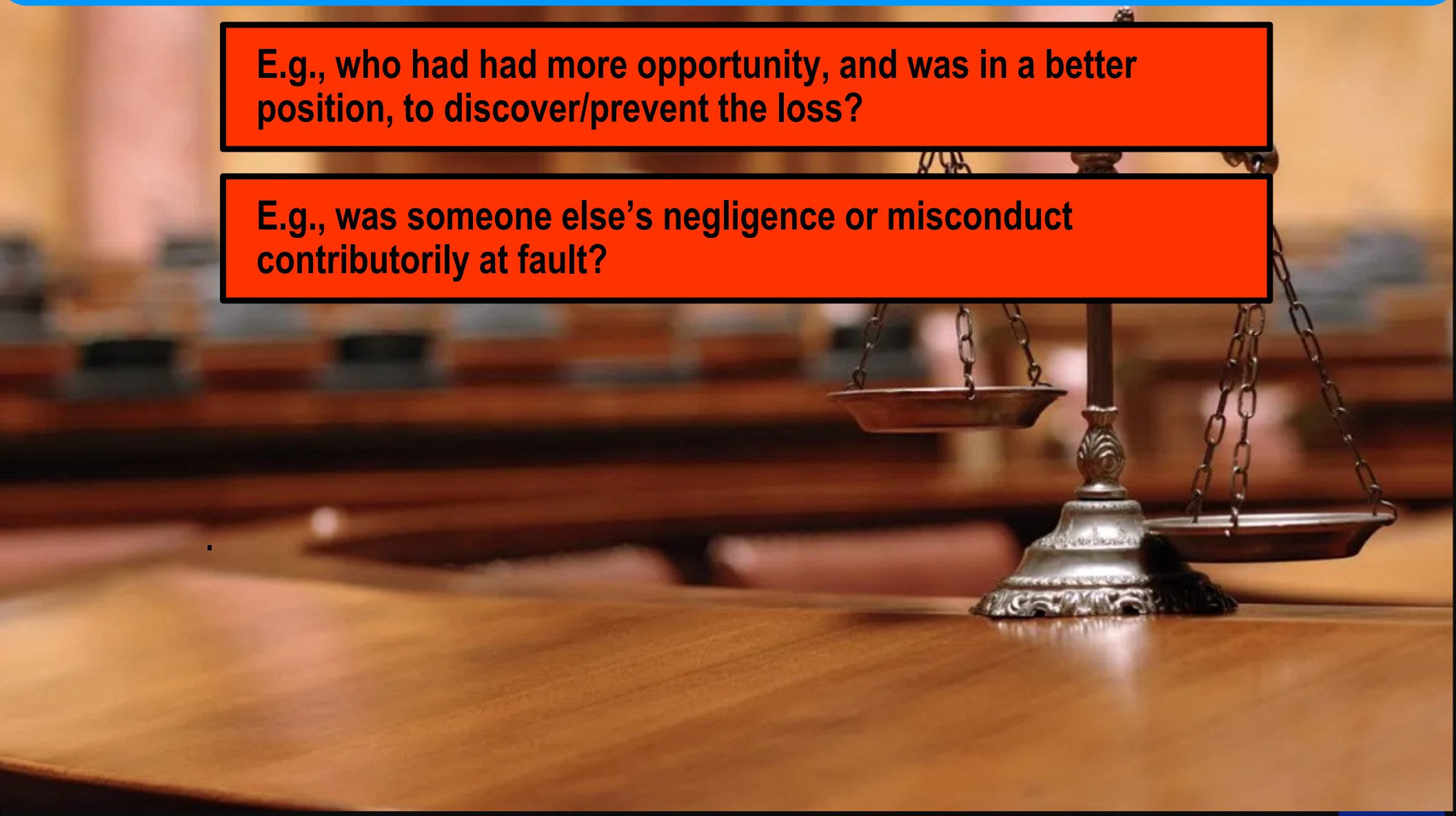
E.g., who had had more opportunity, and was in a better position, to discover/prevent the loss?

Prepare to pursue claims/lawsuits against others fully or partially liable for the loss

E.g., was someone else's negligence or misconduct contributorily at fault?

IMMEDIATELY PREPARE FOR POTENTIAL LITIGATION

[as defendant as well as plaintiff]



E.g., who had had more opportunity, and was in a better position, to discover/prevent the loss?

E.g., was someone else's negligence or misconduct contributorily at fault?

Simplified example: ***Arrow Truck Sales v. Top Quality Truck & Equipment***, (M.D.Fla. 2015) 2015 WL 4936272

- Case involves 12 trucks being sold for $570K
- Buyer (Arrow) routinely bought trucks from seller (Top Quality) by wire transfer
- Email account of seller's sales rep (Joe Gelfo) was joegelfo@gmail.com
- Email account of buyer's rep (Nick Lambardo) was nlombardo@arrowtruck.com
- Cybercrook created two similar email accounts: joegeflo@gmail.com, and nlombardo.arrowtruck.com@gmail.com
- Cybercrook sent buyer and seller emails from these two email accounts – including an email to the buyer with "updated" wiring instructions to a bank account the cybercrook had opened
- Buyer wired the $570K per the "updated" instructions
- Buyer sued seller for not delivering the trucks

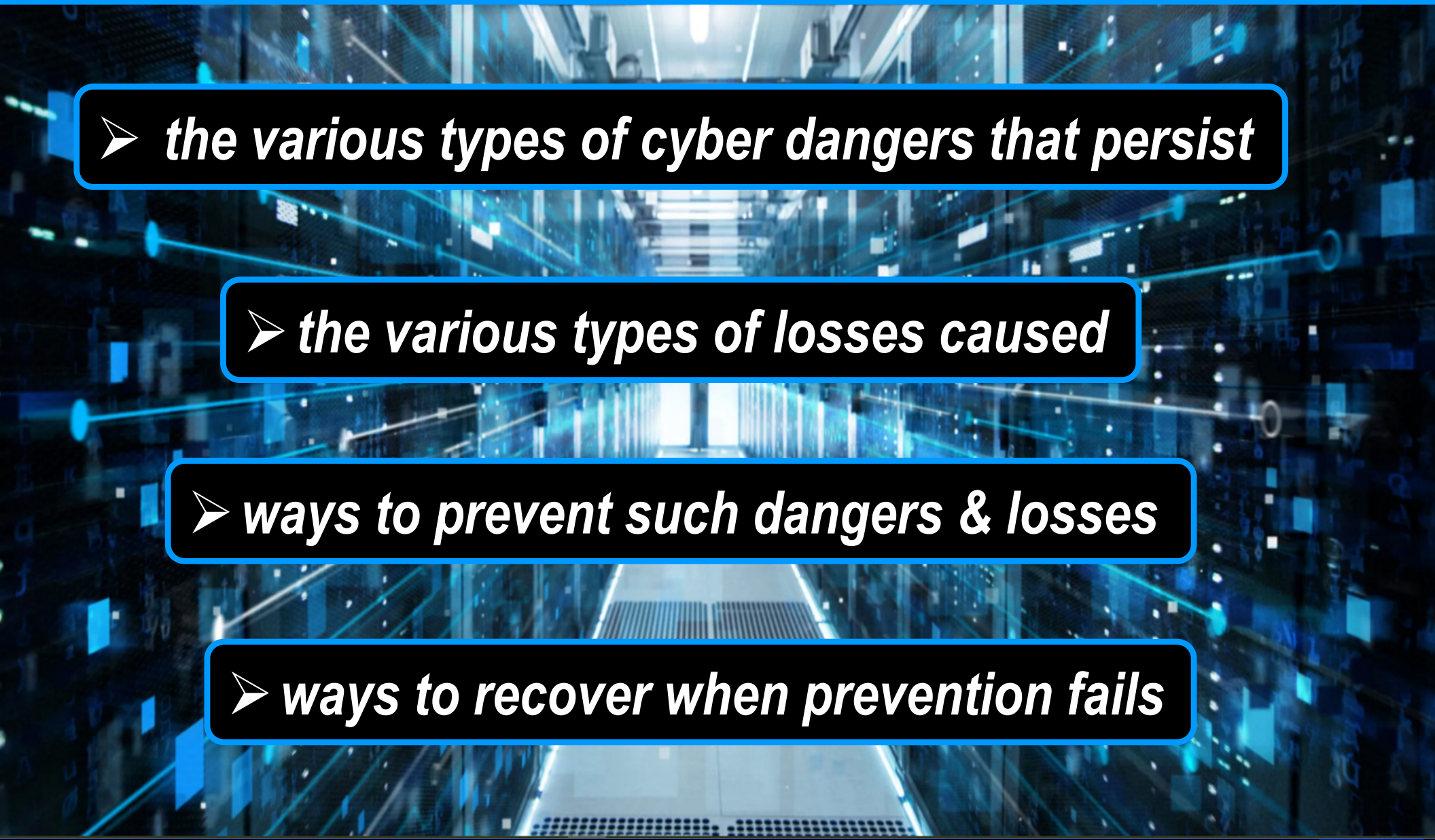
➢ **Court:** Neither buyer nor seller were negligent in the way they maintained their email accounts, and both were victims of sophisticated fraudsters. But ... **buyer bears this loss because it "had more opportunity and was in a better position to discover the fraudulent behavior". Buyer therefore loses its $570K and does not get the trucks.**

Simplified example: ***Beau Townsend Ford v. Hinds Ford***, (6th Cir. 2018) 759 Fed.Appx. 348

- Case involves 20 SUVs being sold for $736K
- Buyer (Hinds) previously bought SUVs from seller (Beau) and paid by check
- Cybercrook hacked into the email account of seller's sales rep, emailed buyer's rep that ""Due to some tax related procedures we will prefer a wire transfer", and emailed wiring instructions for an account the cybercrook had opened.
- To intercept questions from buyer's rep, the cybercrook modified the "rules" in the sales rep's email account to (1) deliver emails from the buyer directly to seller's "deleted items" folder and (2) forward those emails to the cybercrook
- Cybercrook would then put the buyer's email in the seller's inbox, but changed the "sender" from the buyer's actual address (jcolglazier@donhindsford.com) to a similar account the hacker had set up (jcolglazier.donhindsford@gmail.com) so the seller's "reply" email would accordingly go to the cybercrook instead of to the buyer.
- Buyer wired the $736K per the emailed wiring instructions
- Seller sued since seller delivered the SUVs and but did not receive payment.

➢ **Court**: Both buyer and seller were negligent – seller had unsecure email system and buyer failed to confirm wiring change was true. **Between the seller and buyer, this loss falls on the one the factfinder finds "was in the best position to prevent the fraud".** Summary judgment for buyer therefore reversed & remanded for trial.

CYBERCRIME DANGERS FOR PORTS



- the various types of cyber dangers that persist
- the various types of losses caused
- ways to prevent such dangers & losses
- ways to recover when prevention fails


QUESTIONS ???