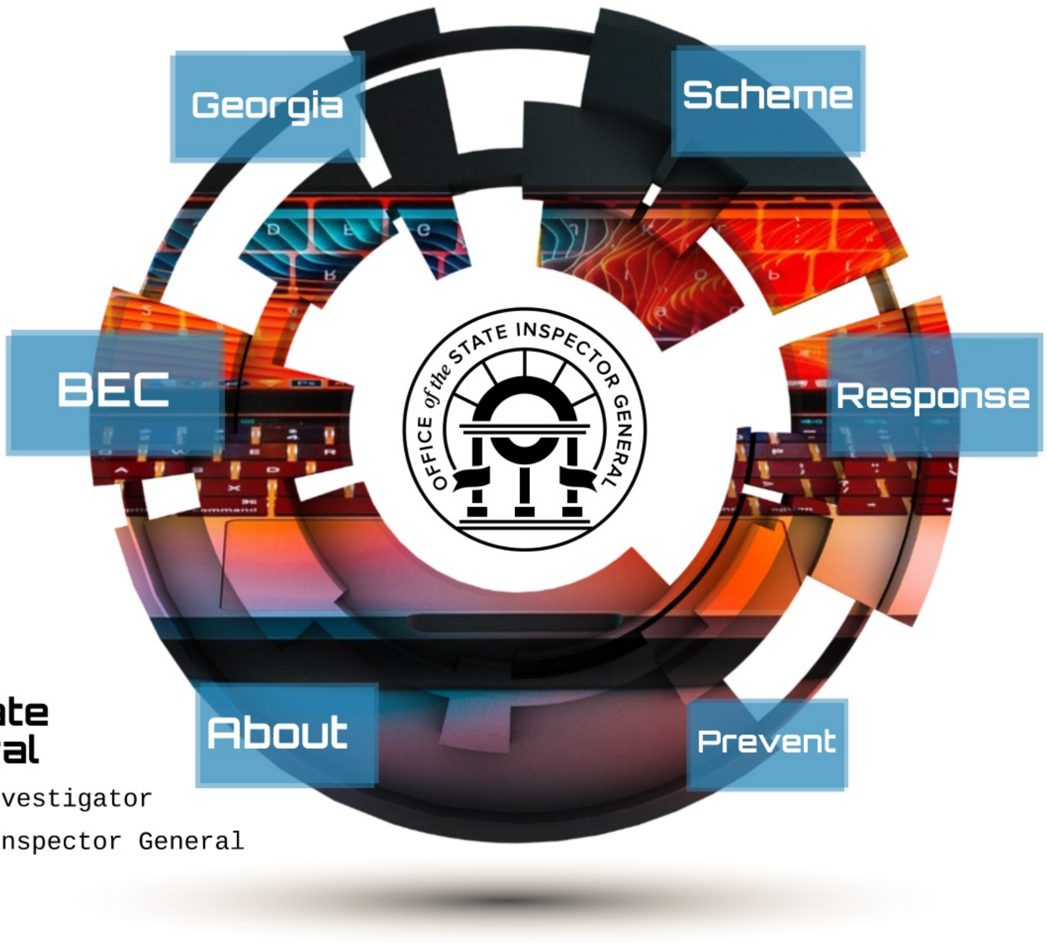


Georgia

Scheme

BEC

Response

About

Prevent

Office of the State Inspector General

Richard Schneider / Investigator

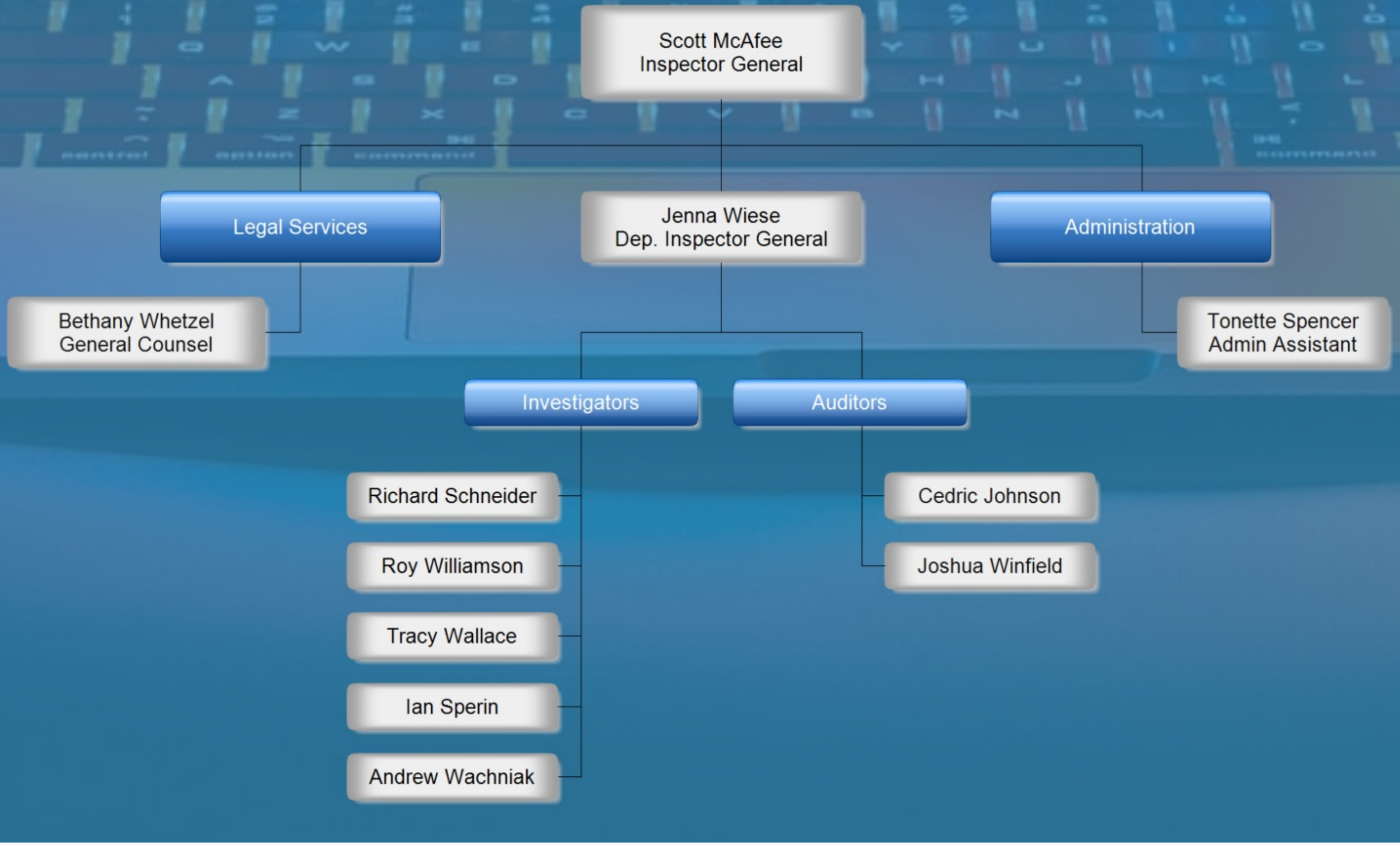
Jenna Wiese / Deputy Inspector General

01/27/2022

State Inspector General

- Created via Executive Order in 2003
- Investigate Fraud, Waste, Abuse, Corruption
- Executive Branch Only
- Jurisdiction Includes State Funds and State Administered Federal Funds
- Administrative -> Criminal, Sexual Harassment

Current Staff



Scott McAfee
Inspector General

Legal Services

Bethany Whetzel
General Counsel

Jenna Wiese
Dep. Inspector General

Investigators

Richard Schneider

Roy Williamson

Tracy Wallace

Ian Sperin

Andrew Wachniak

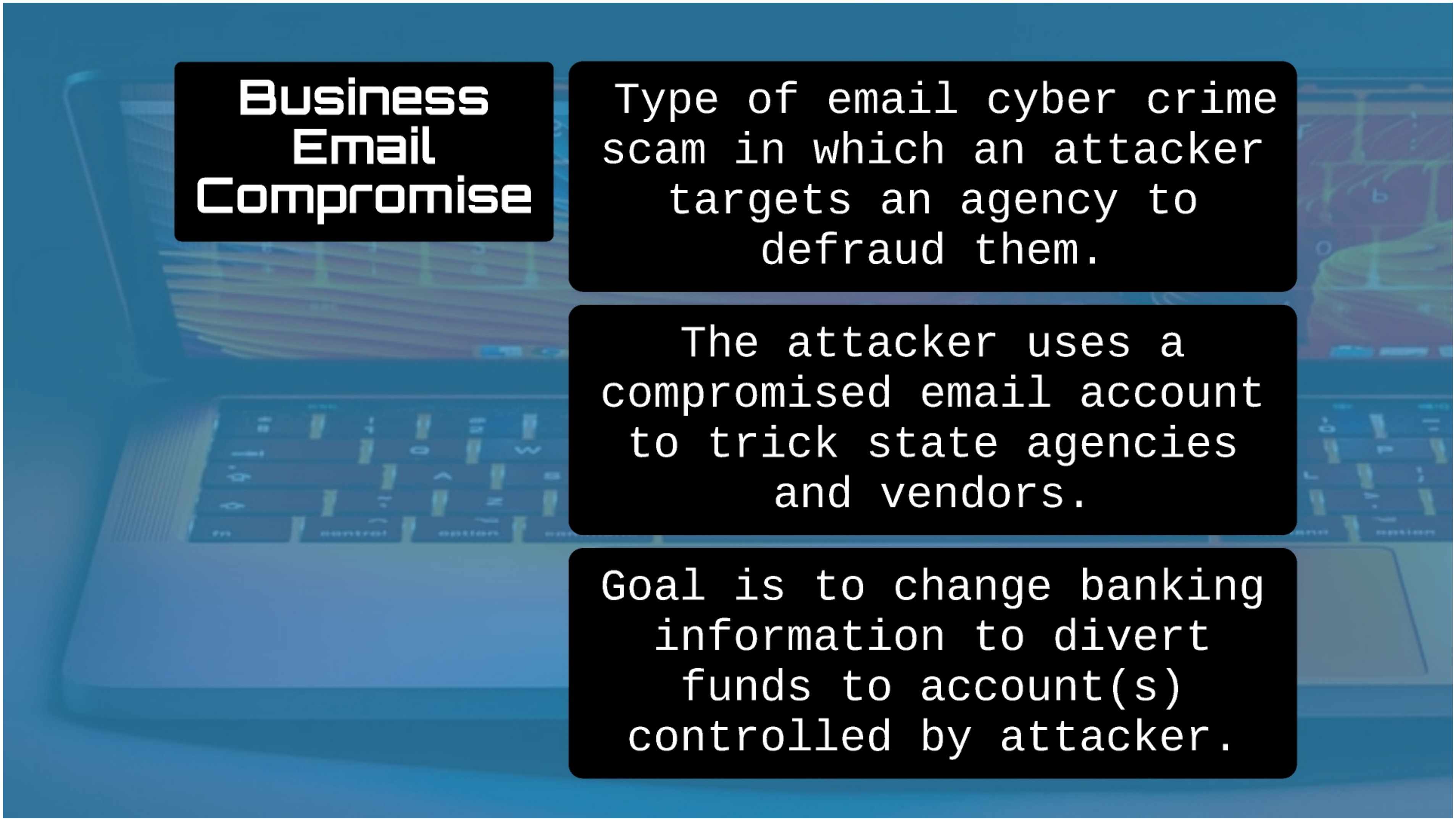
Auditors

Cedric Johnson

Joshua Winfield

Administration

Tonette Spencer
Admin Assistant

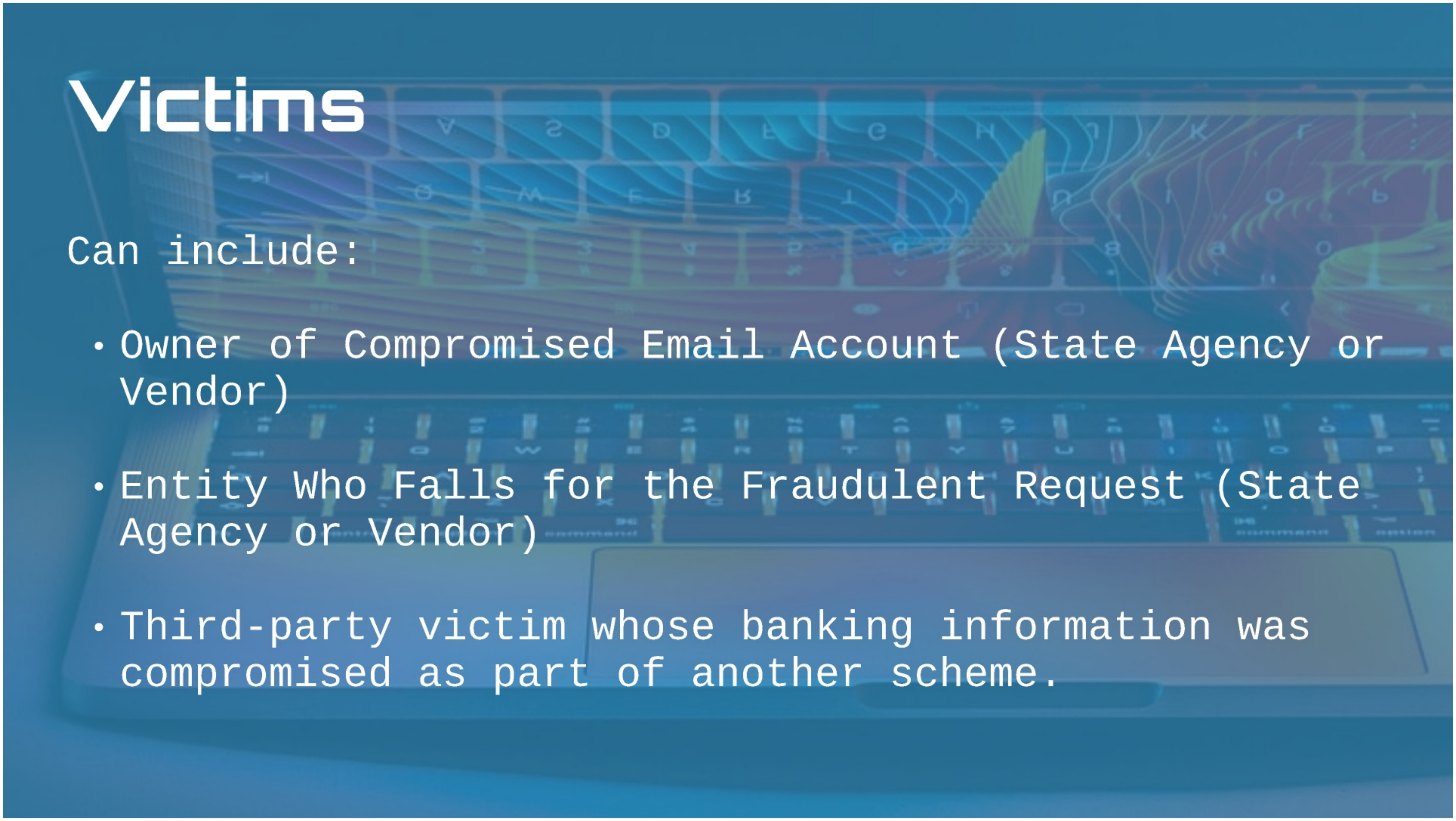


Business Email Compromise

Type of email cyber crime scam in which an attacker targets an agency to defraud them.

The attacker uses a compromised email account to trick state agencies and vendors.

Goal is to change banking information to divert funds to account(s) controlled by attacker.

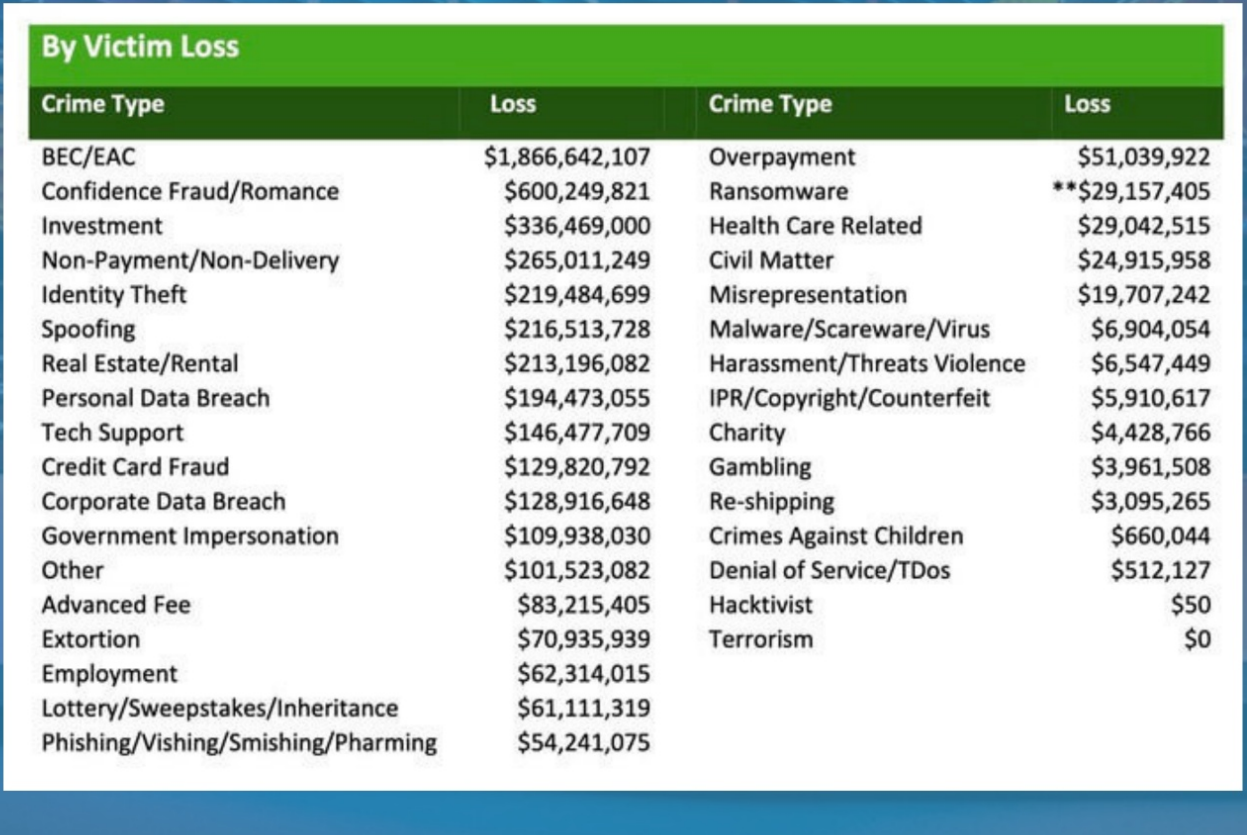


Victims

Can include:

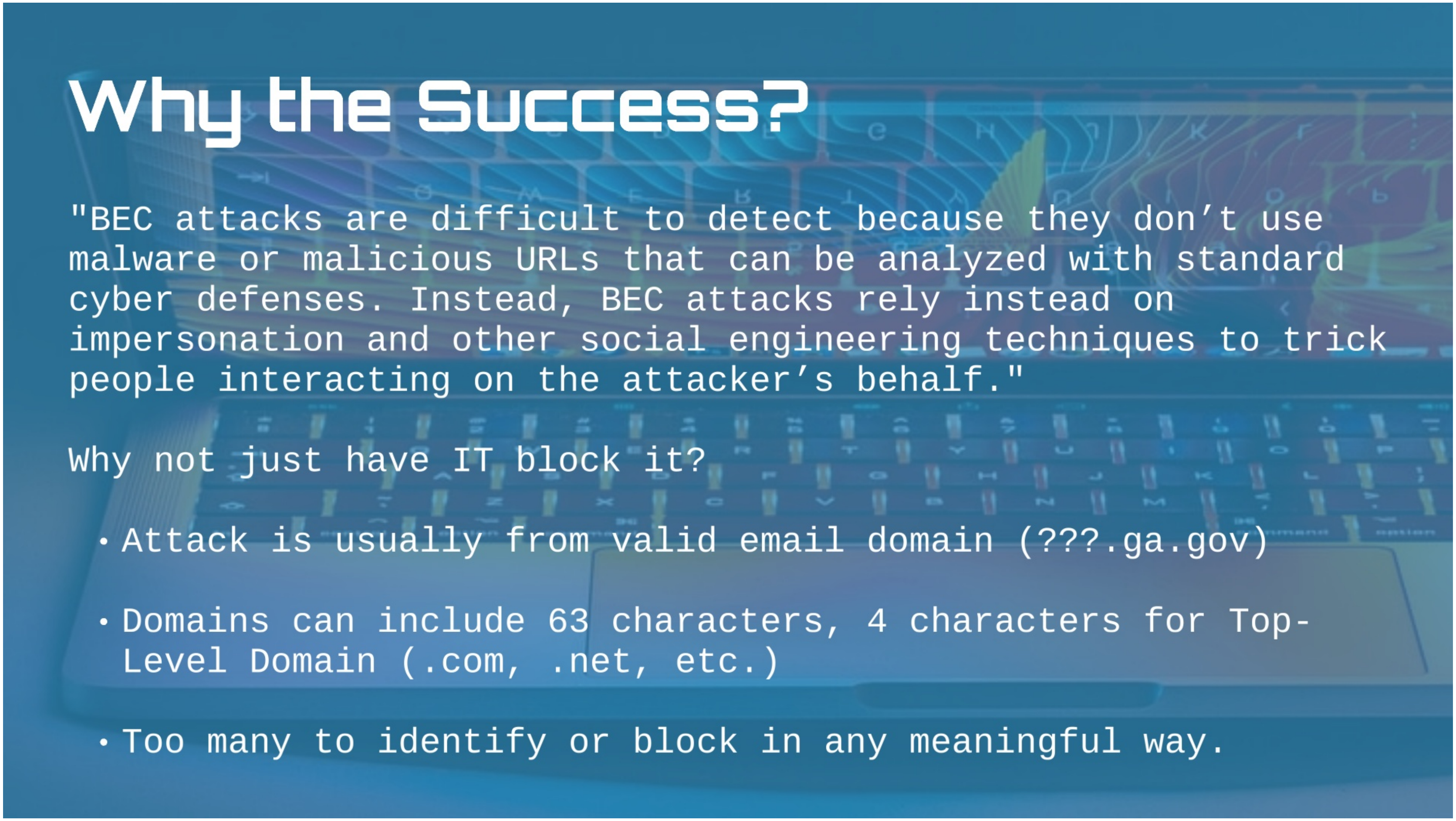
- Owner of Compromised Email Account (State Agency or Vendor)
- Entity Who Falls for the Fraudulent Request (State Agency or Vendor)
- Third-party victim whose banking information was compromised as part of another scheme.

Impact



By Victim Loss

Crime Type	Loss	Crime Type	Loss
BEC/EAC	$1,866,642,107	Overpayment	$51,039,922
Confidence Fraud/Romance	$600,249,821	Ransomware	**$29,157,405
Investment	$336,469,000	Health Care Related	$29,042,515
Non-Payment/Non-Delivery	$265,011,249	Civil Matter	$24,915,958
Identity Theft	$219,484,699	Misrepresentation	$19,707,242
Spoofing	$216,513,728	Malware/Scareware/Virus	$6,904,054
Real Estate/Rental	$213,196,082	Harassment/Threats Violence	$6,547,449
Personal Data Breach	$194,473,055	IPR/Copyright/Counterfeit	$5,910,617
Tech Support	$146,477,709	Charity	$4,428,766
Credit Card Fraud	$129,820,792	Gambling	$3,961,508
Corporate Data Breach	$128,916,648	Re-shipping	$3,095,265
Government Impersonation	$109,938,030	Crimes Against Children	$660,044
Other	$101,523,082	Denial of Service/TDos	$512,127
Advanced Fee	$83,215,405	Hacktivist	$50
Extortion	$70,935,939	Terrorism	$0
Employment	$62,314,015		
Lottery/Sweepstakes/Inheritance	$61,111,319		
Phishing/Vishing/Smishing/Pharming	$54,241,075		

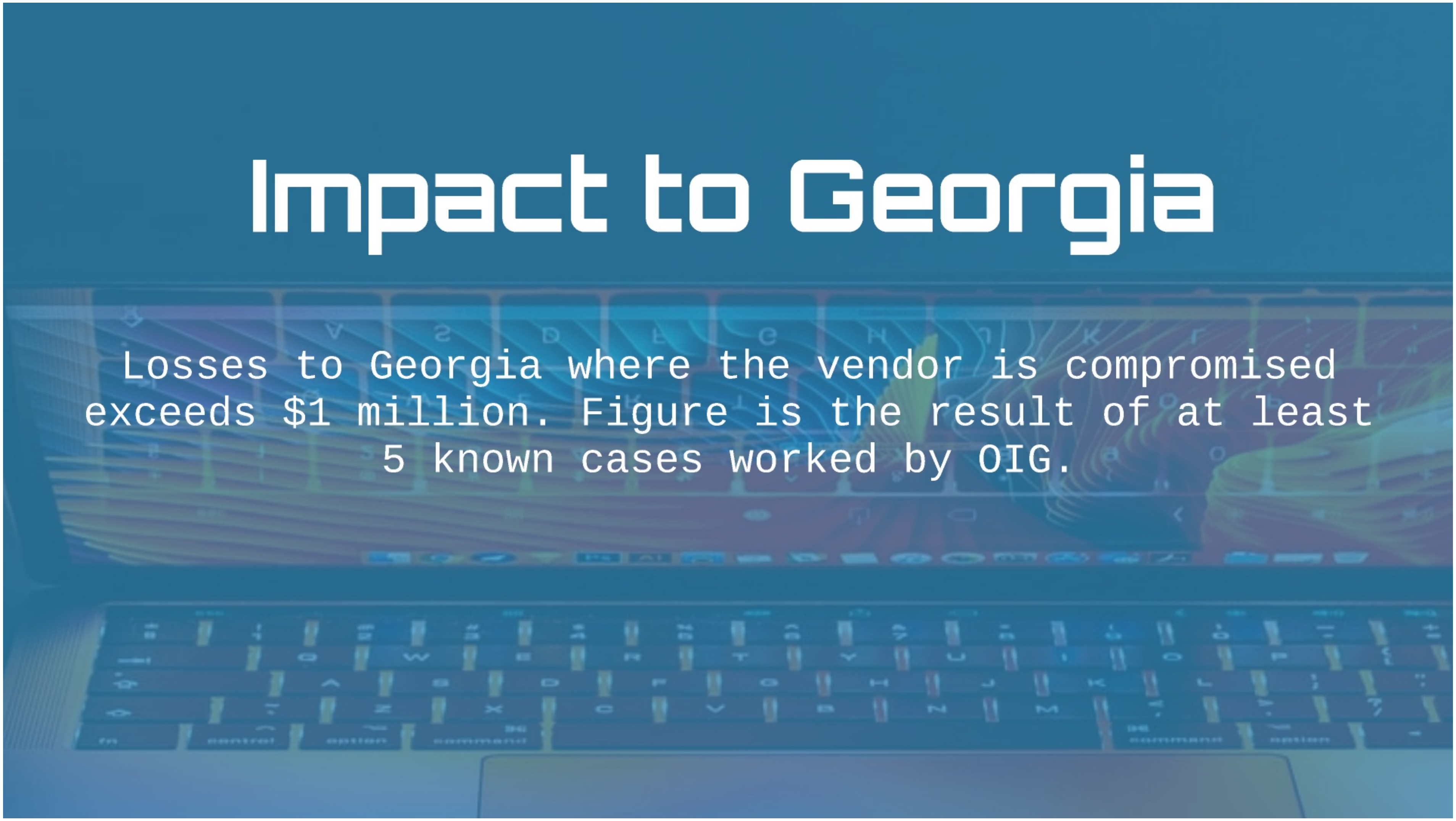


Why the Success?

"BEC attacks are difficult to detect because they don’t use malware or malicious URLs that can be analyzed with standard cyber defenses. Instead, BEC attacks rely instead on impersonation and other social engineering techniques to trick people interacting on the attacker’s behalf."

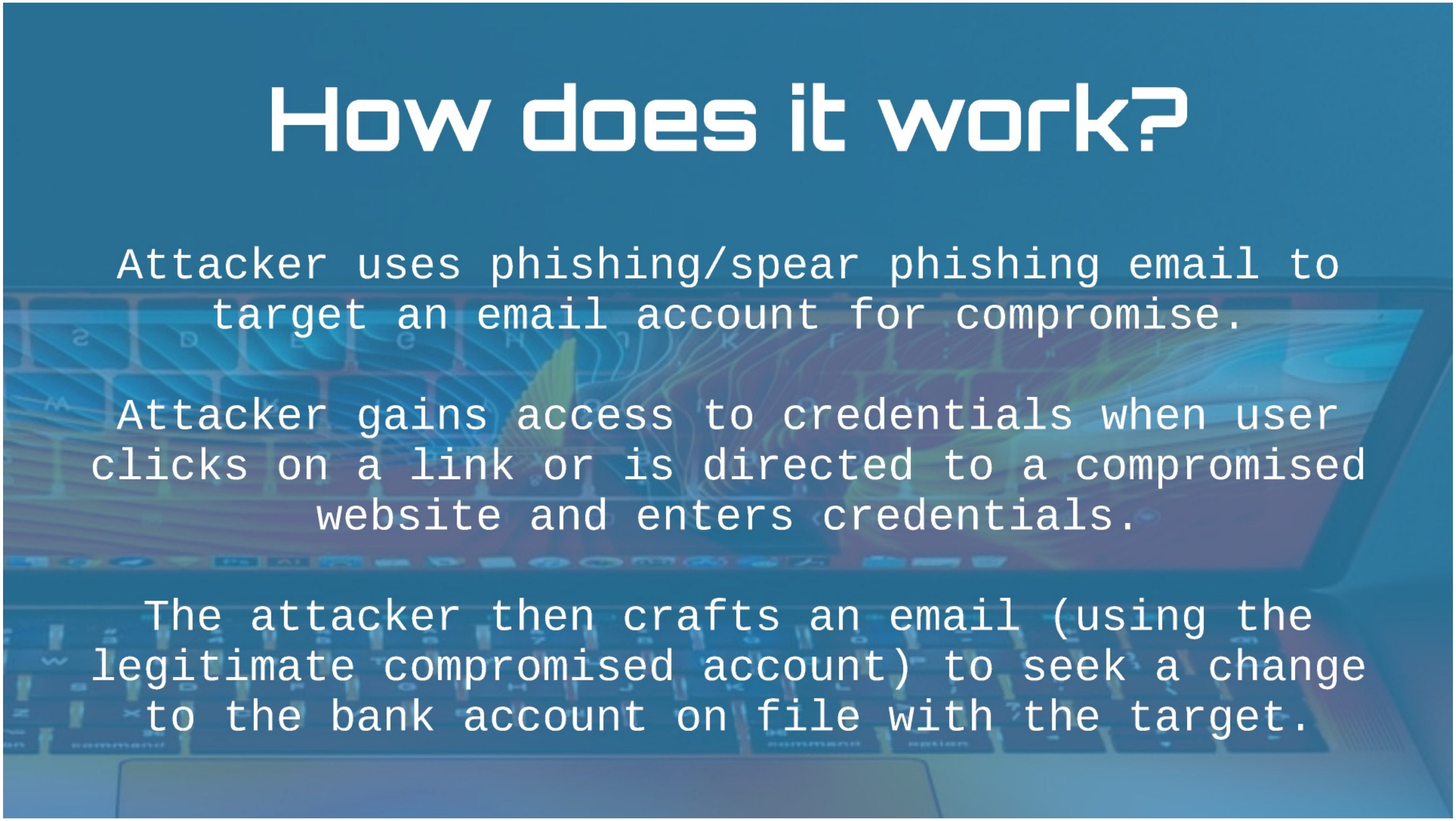
Why not just have IT block it?

- Attack is usually from valid email domain (???.ga.gov)
- Domains can include 63 characters, 4 characters for Top-Level Domain (.com, .net, etc.)
- Too many to identify or block in any meaningful way.



Impact to Georgia

Losses to Georgia where the vendor is compromised exceeds $1 million. Figure is the result of at least 5 known cases worked by OIG.

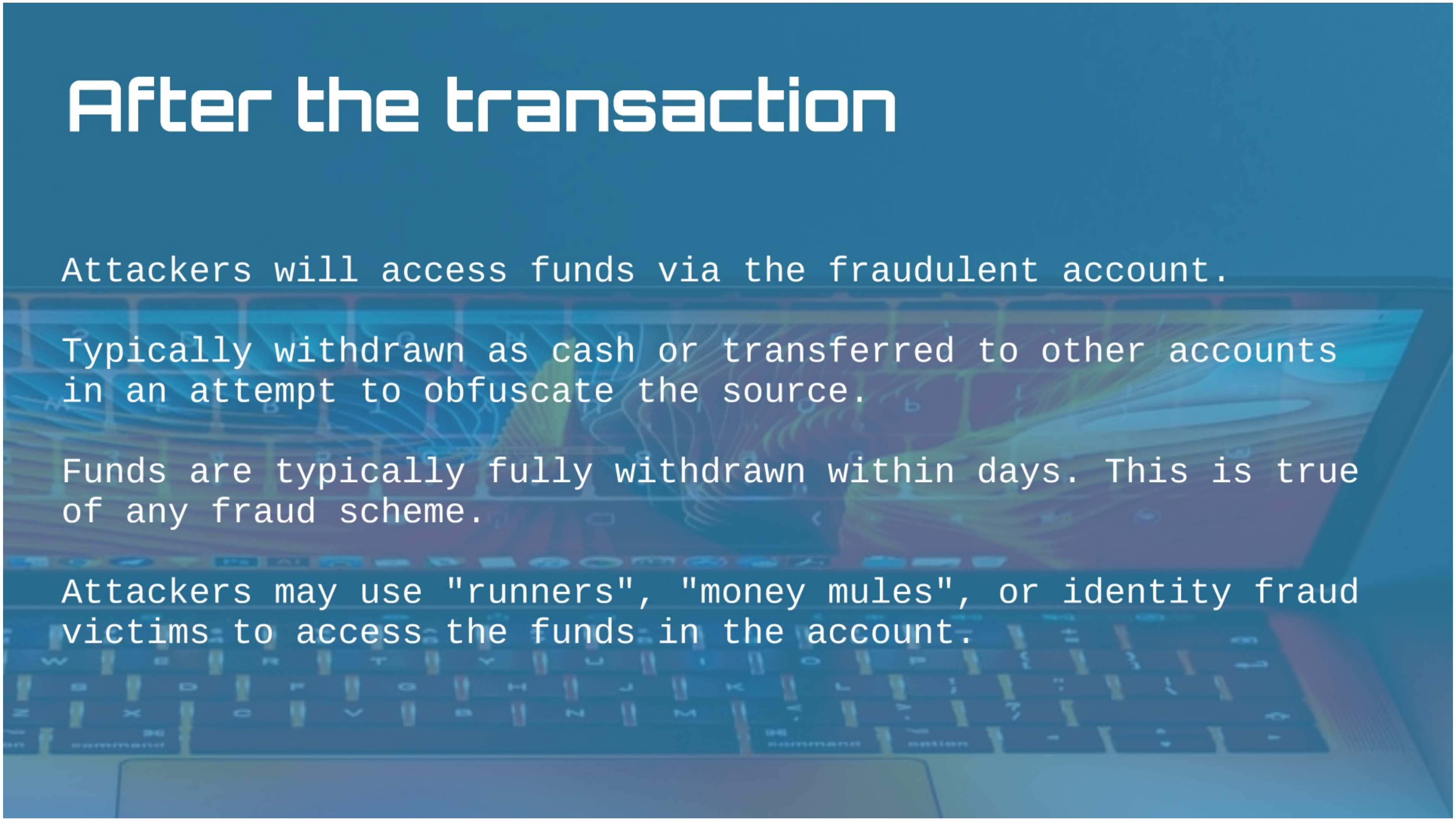


How does it work?

Attacker uses phishing/spear phishing email to target an email account for compromise.

Attacker gains access to credentials when user clicks on a link or is directed to a compromised website and enters credentials.

The attacker then crafts an email (using the legitimate compromised account) to seek a change to the bank account on file with the target.



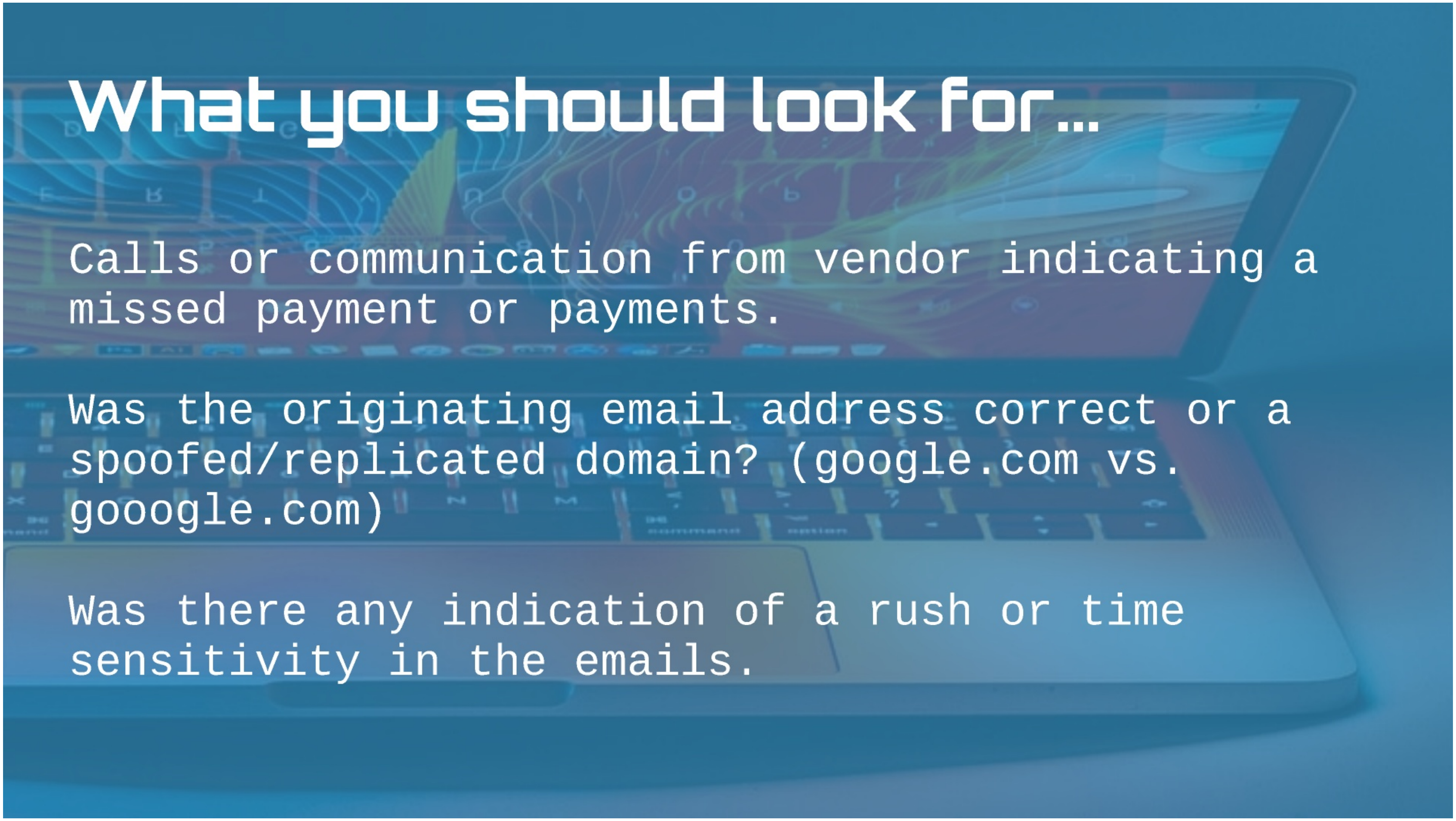
After the transaction

Attackers will access funds via the fraudulent account.

Typically withdrawn as cash or transferred to other accounts in an attempt to obfuscate the source.

Funds are typically fully withdrawn within days. This is true of any fraud scheme.

Attackers may use "runners", "money mules", or identity fraud victims to access the funds in the account.

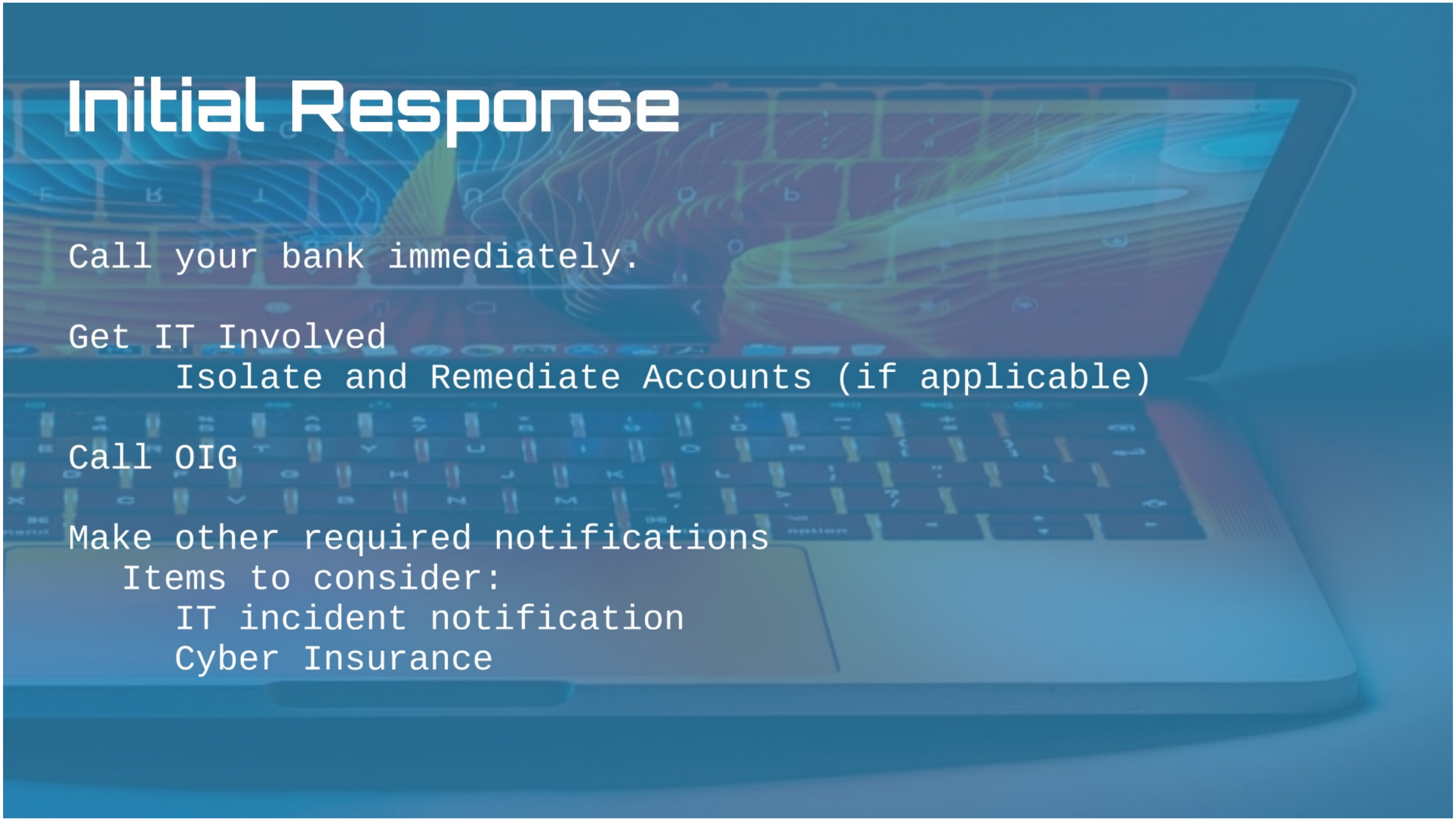


What you should look for…

Calls or communication from vendor indicating a missed payment or payments.

Was the originating email address correct or a spoofed/replicated domain? (google.com vs. gooogle.com)

Was there any indication of a rush or time sensitivity in the emails.



Initial Response

Call your bank immediately.

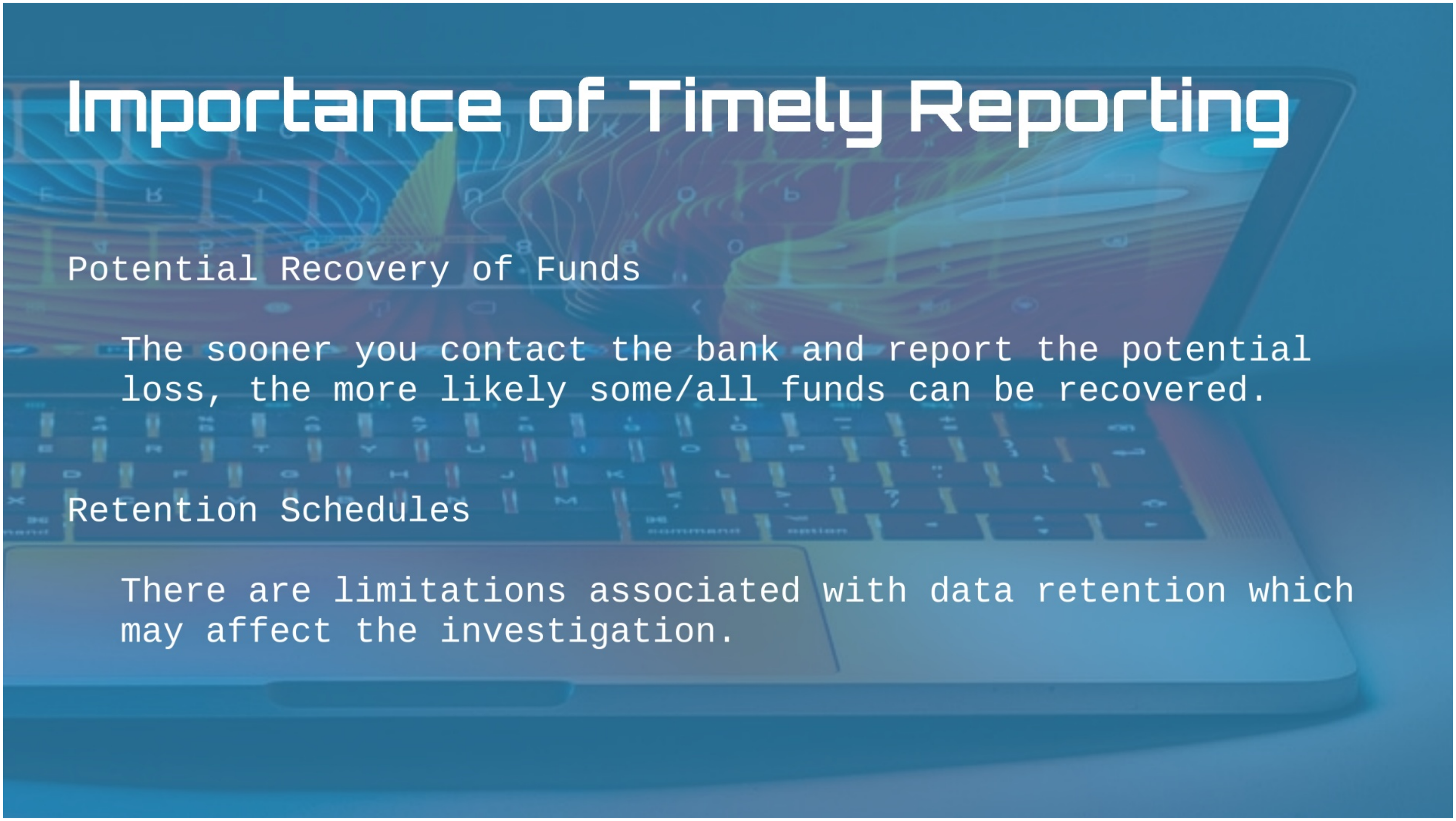
Get IT Involved

- Isolate and Remediate Accounts (if applicable)

Call OIG

Make other required notifications

- Items to consider:
  - IT incident notification
  - Cyber Insurance



Importance of Timely Reporting

Potential Recovery of Funds

The sooner you contact the bank and report the potential loss, the more likely some/all funds can be recovered.

Retention Schedules

There are limitations associated with data retention which may affect the investigation.

Prevention Measures

Two-step or Multi-factor authentication

Education and Training

GIACT or Similar Tool – Verification of account status and name match (financial risk assessment)

Validate Change Outside Email

Automatic Mailings/Notification

Separation of Duties and Documentation

Prevention Measures

Mock-phishing Email Campaigns

State Agencies – Proofpoint

Log Email Changes

Contact Details

Richard Schneider / Investigator
Email: richard.schneider@oig.ga.gov
Work: 404-316-6274

Jenna Wiese / Deputy IG
Email: jenna.wiese@oig.ga.gov
Work: 404-317-6271

OIG Complaint Form: https://oig.georgia.gov/report-fraud-waste-abuse-0

OIG Inbox: ig@oig.ga.gov