Privacy + Security Forum

Session:
Phishing Unveiled: MFA Bypass & Downgrade, Mitigations & Defenses

Privacy+ Security Forum

Speakers: Phishing Unveiled: MFA Bypass & Downgrade, Mitigations & Defenses

Sabrina Guenther Frigo

Chief Ethics, Compliance & Privacy Officer

TruStage

Nathan Salminen

Partner

Hogal Lovells

Kyle Carr

Managing Director

Booz Allen Hamilton

Privacy+ Security Forum

Session: Phishing Unveiled: MFA Bypass & Downgrade, Mitigations & Defenses

Session Agenda

- Business Email Compromise Today
- Phishing Tactics
- MFA Bypass & Downgrade
- Mitigations & Defense
- Lifecycle of an Incident
- Legal Implications
- BEC Scenario / Impact

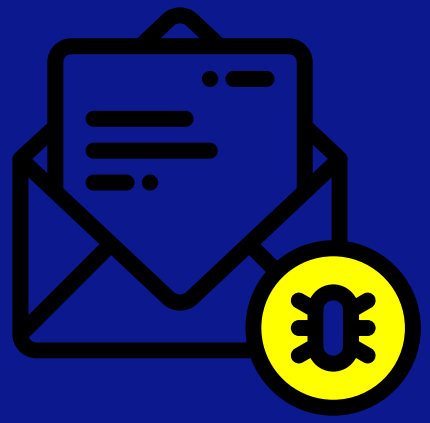
Privacy+ Security Forum

Business Email Compromise Today

Statistics issued via the FBI's Internet Crime Complaint Center and derived from financial institutions between 2013 and 2025. BEC holds strong as #2 for total monies lost from a cyber incident, only being beat by Crypto fraud, not including cost of investigation, legal fees or data mining/notification.

~349,475

Domestic and international incidents reported between October 2013 and December 2025



81%

Percentage of victims in the United States between October 2013 and December 2025

As of 2023: $55,499,915,582

2024: ~(+2.8b) $58,299,915,582

2025: ~(+3.5b) $61,799,915,582

Domestic and international exposed dollar loss between October 2013 and December 2025

67%

($41,405,943,439)

Percentage of total exposed dollar loss reported by victims in the United States between October 2013 and December 2025

Privacy+ Security Forum

Business Email Compromise Today

BEC Statistics

Business Email Compromise

- 2025 - 800+ Cases last year
  - 69% – M365
  - 13% – Google Workspace
  - 10% – Other (AOL, Yahoo, etc)
  - 6% – Exchange
  - 1% – Hybrid Exchange
- 30% Data Mining Quotes

Was MFA in Place Prior to the Event?

82% *"Yes"*

18% *"No"*

What MFA was in Place?

SMS Text
Call
Email Code
MS Authenticator
GW Authenticator
Okta
DUO

Privacy+ Security Forum

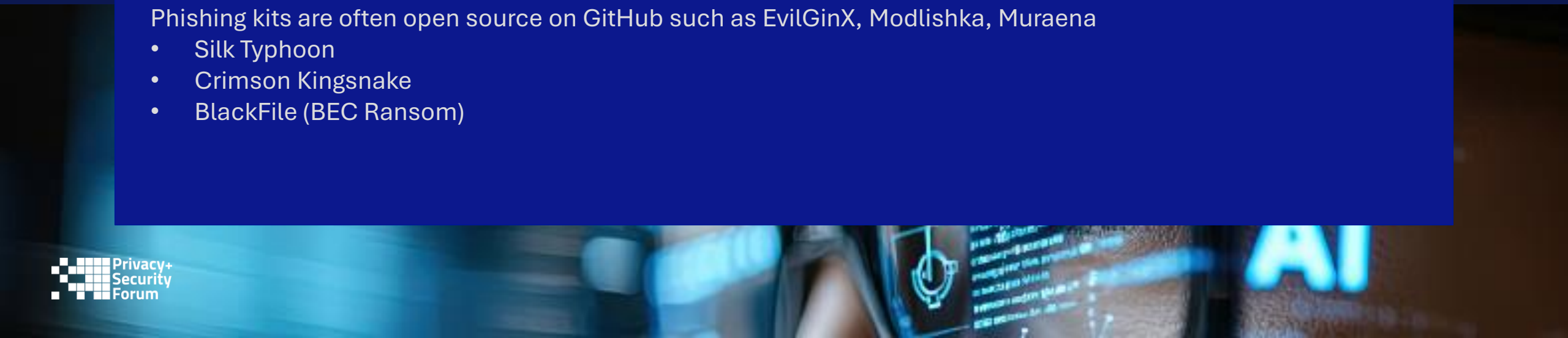
Phishing Tactics

The goal of a threat actor is to get a victim to click on a link and provide their credentials to a site that they believe to be legitimate.

- Phishing link inside of email – often from a known vendor/partner
- Notification from a legitimate platform (SharePoint, Dropbox, DocuSign)
- Phishing link inside an attachment (Word, PDF, .HTML)
- Phone Call pretending to be IT Support
- Social Media Advertisements
- AI for Deepfake Voices and Impersonation

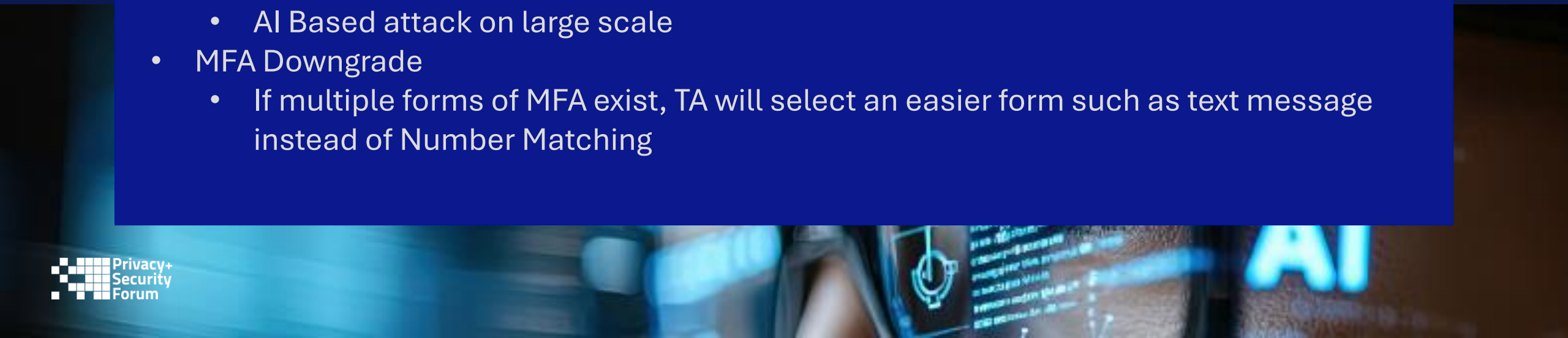
Phishing kits are often open source on GitHub such as EvilGinX, Modlishka, Muraena

- Silk Typhoon
- Crimson Kingsnake
- BlackFile (BEC Ransom)



MFA Bypass & Downgrade

- Legacy Protocols – IMAP4, POP3, SMTP
  - MFA cannot support these authentication requests and will bypass MFA
- Register Fraudulent Enterprise Application
  - Phishing page requests user to approve a new enterprise application permissions
- Adversary in the Middle
  - Phishing page requests credentials + MFA token
- EvilToken
  - Phishing page requests you register the threat actor's device
  - AI Based attack on large scale
- MFA Downgrade
  - If multiple forms of MFA exist, TA will select an easier form such as text message instead of Number Matching



BEC Attack Outline

Victim Receives Phishing Email

- May come from a legitimate vendor or known source.
- Common disguises are Docusign, Dropbox, SharePoint, Voicemails and QR Codes

User Visits Phishing Page

- Phishing Site will look identical to legitimate logon page and ask for the Username and Password
- In real time the phishing page will try to log into the legitimate email site
- If the email site asks for an MFA code, the phishing will ask the user for their MFA code as well.

MFA Bypass

- Phishing Site can mimic all digital MFA requests including SMS, Call & Authenticator Applications
- Once the MFA code is put into the phishing site, it will generate a Session Token
- Threat Actor can copy the token out of the phishing and into M365 to bypass MFA

Persistence

- Add additional MFA
- Register an M365 Enterprise Application with Secret Keys
- Secretly search all emails for financial data
- Create inbox rules to hide legitimate conversations with vendors

Attack

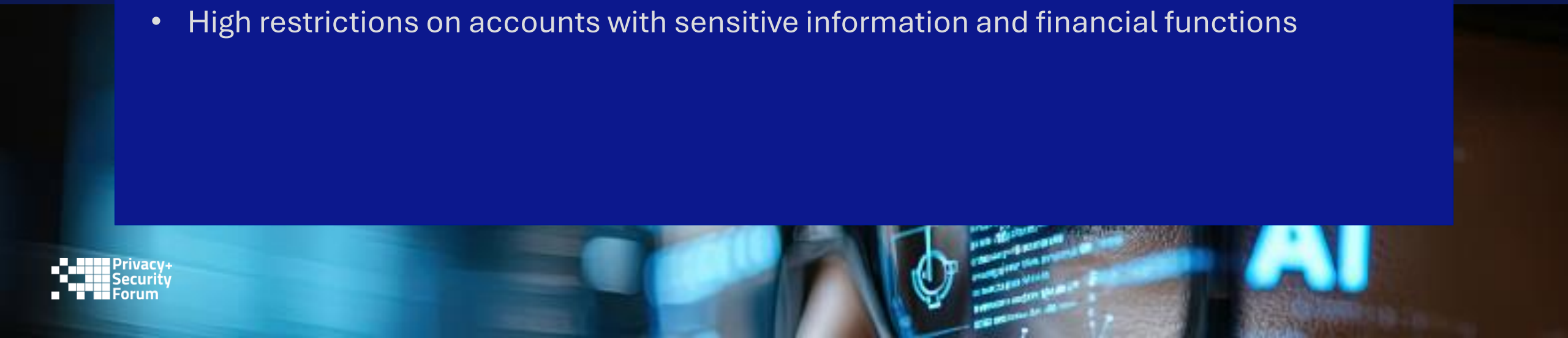
- Identify an upcoming payment and Redirect a Wire Transfer
- Mine all Contact contacts in the mailbox
- Send mass phishing emails
- Exfiltrate full contents of the mailbox

Privacy+ Security Forum

Mitigations & Defenses

Mitigations

- User Training
  - Identifying phishing emails, URLs, domains
- MFA Enabled & **Enforced**
- Understanding proper procedures for remediation
- Disable Legacy Authentication
- Alerting on Impossible Travel & suspicious inbox rules
- Restriction of accounts with Administrative permissions
- High restrictions on accounts with sensitive information and financial functions



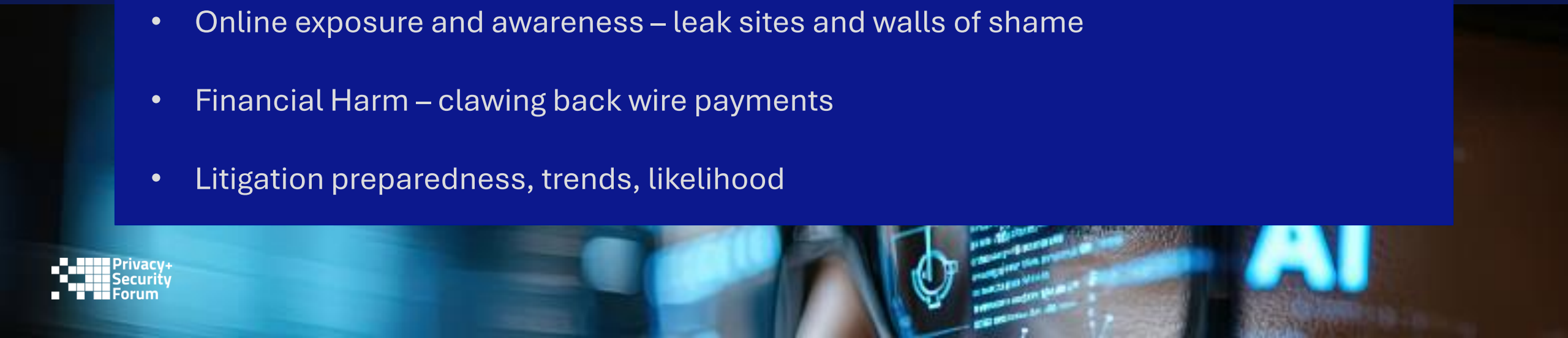
Mitigations & Defenses

Defenses

- Spam filtering products
- Fast Identity Online Alliance (FIDO) and FIDO2 Methods
  - Biometric, Face ID, Touch ID, Windows Hello
  - YubiKey, Smart Card, Device Certificate
- Conditional Access Policies (M365) / Context Awareness Policies (Google Workspace)
  - Your cloud license is probably already paying for these
  - Geolocation Restriction
  - IP Restriction
  - Device Restriction
  - Require IT Team to approve new devices/applications
- Managed Detection and Response products for 24x7 monitoring

Legal Implications

- Notification/Communication Considerations
  - Downstream phishing awareness
  - Regulatory Requirements
- Data Mining Considerations
  - User mailbox information access
  - Timelines
- Online exposure and awareness – leak sites and walls of shame
- Financial Harm – clawing back wire payments
- Litigation preparedness, trends, likelihood

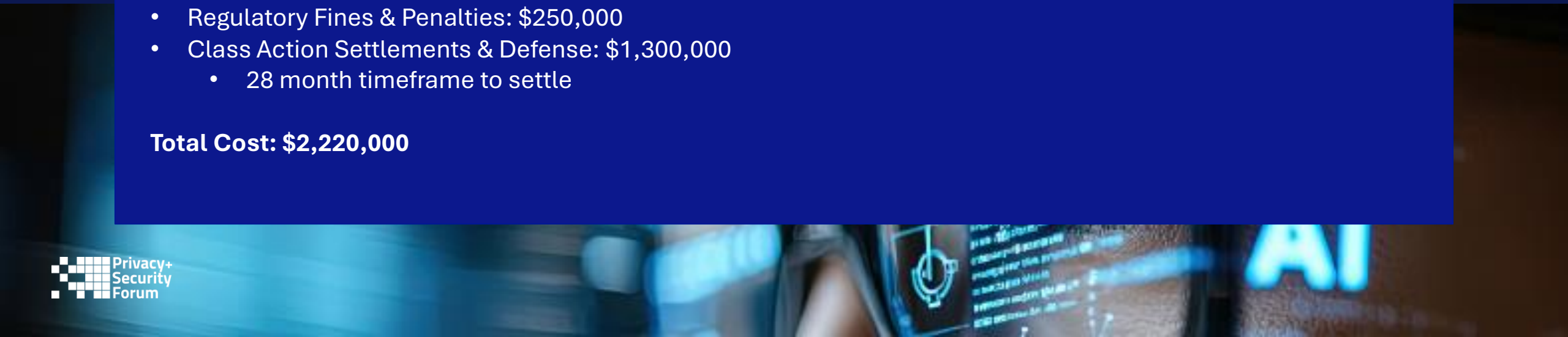


BEC Scenario & Impact

Assumptions: M365 tenant with 2,500 users, 3 accounts compromised and a total compromised dataset of 100 GBs including PCI, PHI and PII data across multiple jurisdictions in the United States only.

- Booz Allen BEC Forensic Investigation: $10,000
- Data Mining & Manual Review: $200,000
- Legal Fees: $50,000
- Notification Expenses (Paper Mailings, etc): $15,000
- Call Center Services: $5,000
- Credit Monitoring: $10,000
- PCI Fines & Penalties: $380,000
- Regulatory Fines & Penalties: $250,000
- Class Action Settlements & Defense: $1,300,000
    - 28 month timeframe to settle

Total Cost: $2,220,000



Stay in touch: Continue the conversation with us

Sabrina Guenther Frigo
TruStage
sabrina.guentherfrigo@trustage.com

Nathan Salminen
Hogan Lovells
nathan.salminen@hoganlovells.com

Kyle Carr
Booz Allen Hamilton
carr_kyle@bah.com

Privacy+ Security Forum