STIFEL BANK TREASURY CLIENT BRIEFING

# The AI Jungle

## How to operate your business safely in the age of AI Fraud

**Cy Khormaee**

Co-founder & CEO, AegisAI

AegisAI

**AI ATTACKS & FRAUD** · *a briefing for the people who move the money*

ABOUT ME

# I've spent my career on the defending side of the inbox.

GOOGLE

### Google User Protection

reCAPTCHA, Safe Browsing and Web Risk — the systems that warn billions of devices about phishing and malware.

AEGISAI

### Co-founder & CEO

Our founding team left Google to build the first AI lab for email security - AI agents that investigate every message.

UCLA

### AI Faculty

I developed and teach the AI and digital transformation classes at the UCLA Anderson School of Management



Accel Battery foundation capital

**CY KHORMAEE** · *cy@aegisai.ai*

AegisAI

THE PROBLEM

# Find the one bad payment.

Treasury sits under a waterfall of transactions. Hundreds are routine. One is a fraud that looks exactly like the rest.

You have to be right every time. The attacker has to be right once.

| OUTGOING PAYMENTS · TODAY | | | 412 QUEUED |
|---|---|---|---|
| 8:52 | Harbor Logistics | ACH | $38,410.00 |
| 8:57 | Payroll funding | Wire | $1,204,882.17 |
| 9:03 | Kestrel Packaging | ACH | $12,950.00 |
| 9:08 | State tax deposit | ACH | $96,300.00 |
| **9:14** | **Northwind Supply** | **Wire** | **$482,150.00** |
| *Fraud · bank details "updated" by email two days ago* | | | |
| 9:21 | Atlas Insurance | Wire | $71,665.40 |
| 9:26 | Meridian Leasing | ACH | $24,000.00 |
| 9:31 | Intercompany sweep | Book | $3,500,000.00 |
| 9:35 | Brightline IT Services | ACH | $8,742.19 |

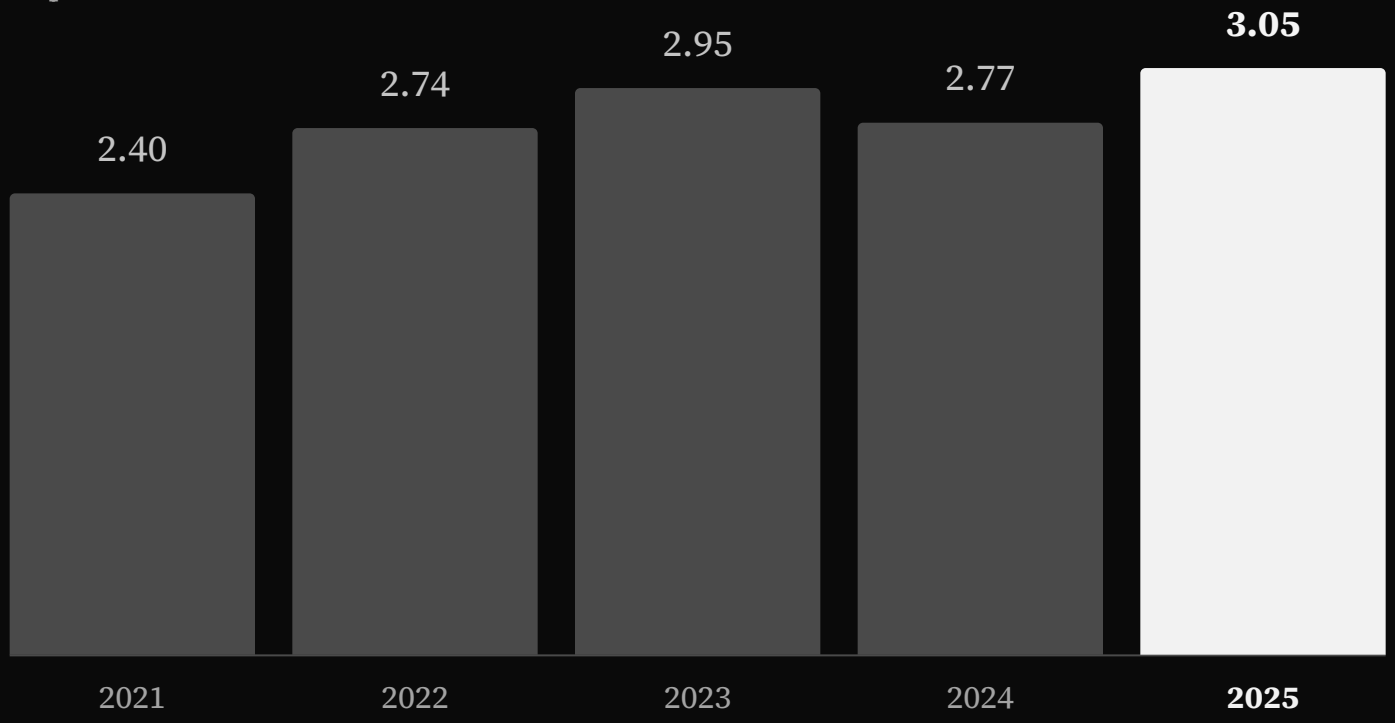
**ILLUSTRATIVE** · *payees and amounts are fictional*

AegisAI

FBI DATA · BUSINESS EMAIL COMPROMISE

# BEC is a $3 billion-a-year line item.

Reported BEC losses, US, $ billions




**$13.9B**
lost to BEC in the last five years — reported cases only

**~$123K**
average loss per BEC complaint in 2025 (24,768 complaints)

**#2**
costliest cybercrime type in 2025, behind investment fraud

**SOURCE** · *FBI IC3 Internet Crime Reports, 2021–2025*

AegisAI

YOUR PEERS · AFP PAYMENTS FRAUD SURVEY

# Three in four finance teams were targeted last year.

**76%**
of US organizations saw attempted or actual payments fraud in 2025

**74%**
were hit by business email compromise — up from 2023 and 2024

**25%**
saw fraud aimed at their wires; checks (58%) and ACH debits (30%) too

**17%** **of organizations use AI to fight payments fraud. The attackers already do.**

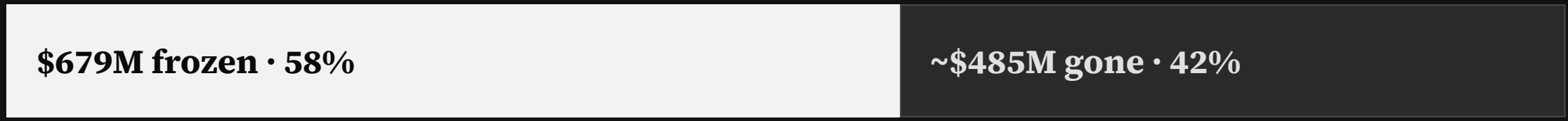
**SOURCE** · *2026 AFP Payments Fraud and Control Survey (2025 data)*

AegisAI

FBI DATA · GETTING MONEY BACK

# Speed is the only recovery plan.

FBI Financial Fraud Kill Chain, 2025 · 3,900 incidents · $1.16B attempted




### Minutes

Call your bank’s fraud line first. Ask for a recall on the wire.

### Hours

File at ic3.gov with the wire details so the FBI can work the receiving bank.

### Days

Funds are moved, split and converted. Recovery odds fall fast.

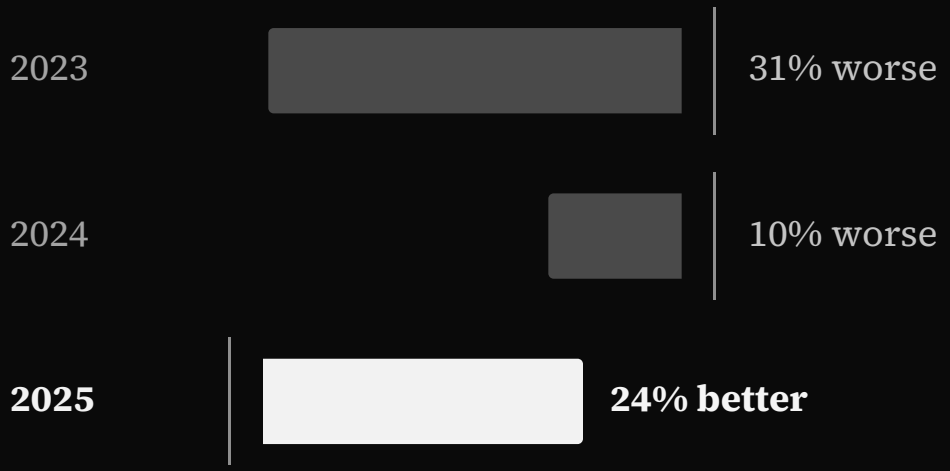
**SOURCE** · *FBI IC3 2025 Internet Crime Report, Recovery Asset Team*

AegisAI

WHY PHISHING BECAME RAMPANT

# AI now out-phishes the experts.

AI spear phishing vs. elite human red team — click effectiveness




*Hoxhunt experiments, 2023 – March 2025*

**82.6%**
of phishing emails studied used AI (Sept 2024 – Feb 2025)

**54%**
click rate for fully AI-run spear phishing, at 95%+ lower cost

**$893M**
2025 losses in FBI complaints that involved AI

**SOURCES** · *Hoxhunt; VIPRE / Keepnet; Heiding, Schneier et al. (HBR 2024); FBI IC3 2025*

AegisAI

PHISHING TRAINING, REVISITED

# Most of the old red flags are gone.

| WHAT TRAINING TAUGHT YOU | WHY IT FAILS NOW |
|---|---|
| ~~Look for typos and bad grammar~~ | AI writes flawless, on-tone prose in any language. |
| ~~Check the sender's address~~ | It comes from a real, compromised vendor mailbox. |
| ~~Beware generic greetings~~ | AI knows your name, your deals and your vendors. |
| ~~Distrust urgent notes from strangers~~ | It arrives inside an existing thread, from someone you know. |
| ~~Call the number in the email~~ | A cloned voice answers. Call a number you already had. |

**THE NEW RULE** · *judge the request, not the writing*

AegisAI

PRIVATE WEALTH & TREASURY

# You are who they're looking for.

### Money in motion

Large, routine payments — the exact shape a fraud copies.

### A public footprint

Filings, LinkedIn, press and board bios feed the AI.

### Many trusted parties

Vendors, advisors, attorneys, escrow agents — every inbox is a way in.

### Authority to approve

One approval moves the money. They target you — or your assistant.

**$7.7** **lost by Americans 60 and over in 2025 — the most of any age group. Investment fraud led all categories at $8.6B.**

**SOURCE** · *FBI IC3 2025 Internet Crime Report*

AegisAI

LIVE DEMO

# 60 seconds to a perfect fraud email.

1. Paste in public info: a company site, a LinkedIn page, a press release.
2. Ask for a vendor note about new bank details, in a real person's voice.
3. Find the red flag. There isn't one.

From: **Dana Whitfield, Northwind Supply**
Subject: **Re: Q4 remittance — updated banking details**

Hi Mark,

Thanks again for turning around INV-88213 so quickly. Quick heads-up as we close the quarter: following our move to a new treasury bank, our remittance details have changed. The updated instructions are on our letterhead, attached.
Could you apply them before Friday's payment run? Our old account closes at month-end.

Best, Dana

**Written by AI in seconds · no typos, no links, a real invoice number**

**ILLUSTRATIVE** · *fictional company and people*

AegisAI

WHAT WE SEE NOW

# Six attacks training didn’t cover.

### Vendor takeover
The attacker sits in your real vendor’s mailbox and replies in your real thread.

### Deepfake executive
A cloned voice or video “CFO” approves the wire. One firm lost $25M on a single call.

### One-of-one phishing
AI researches each target and writes a unique email for every person, at scale.

### MFA bypass
A fake login page relays your code and steals the live session to your inbox or bank portal.

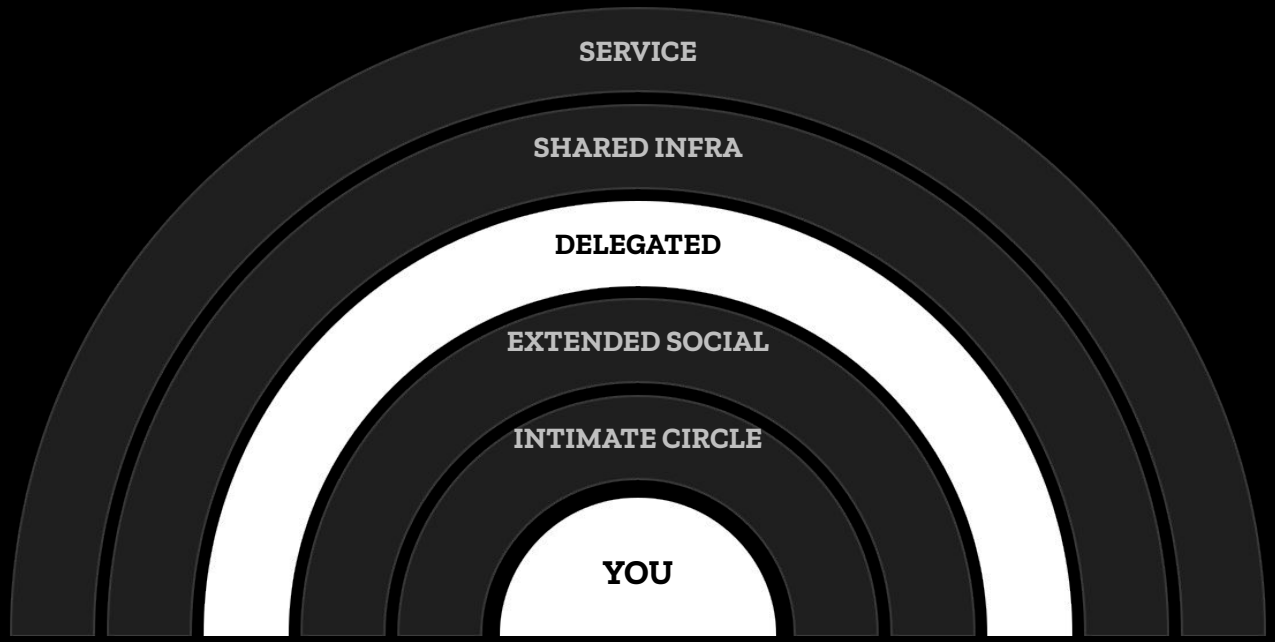
### Callback scams
No link at all — just a phone number and a “bank fraud team” that talks you through it.

### QR code phishing
A code in an email or PDF moves the attack to your phone, outside company protection.

**COMMON THREAD** · *each one looks legitimate to a person*

AegisAI

# Your perimeter: anyone who can say “it’s me”




**Service relationships** — NONE

Carrier, personal email, bank, school portal

**Shared infrastructure** — NONE

Home router, shared cloud, media servers

**Delegated professional** — PARTIAL

Advisor, attorney, accountant, assistant

**Extended social** — NONE

Close friends, neighbors, alumni groups

**Intimate circle** — NONE

Spouse, children, parents, live-in staff

***Your bank and employer protect one ring of five.***

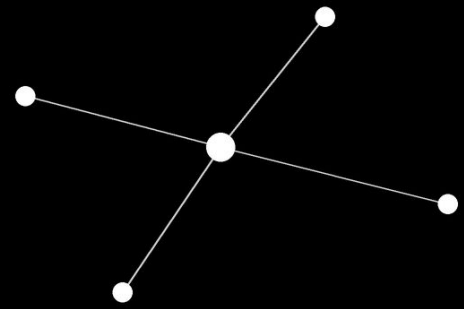


AegisAI

# The calendar invite that spreads itself

**4**

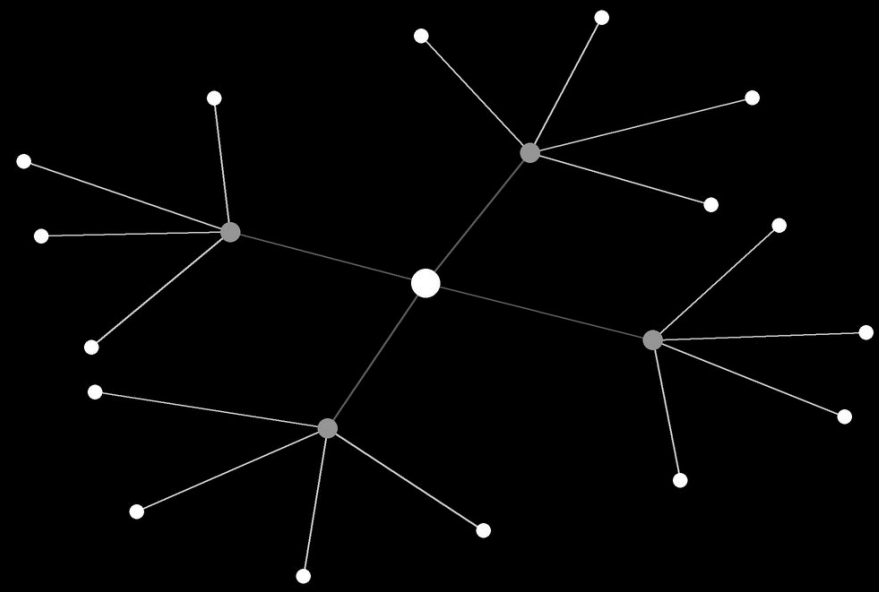
Each victim’s mailbox
becomes the next sender.



# The calendar invite that spreads itself

**16**

Every wave recruits the next one.

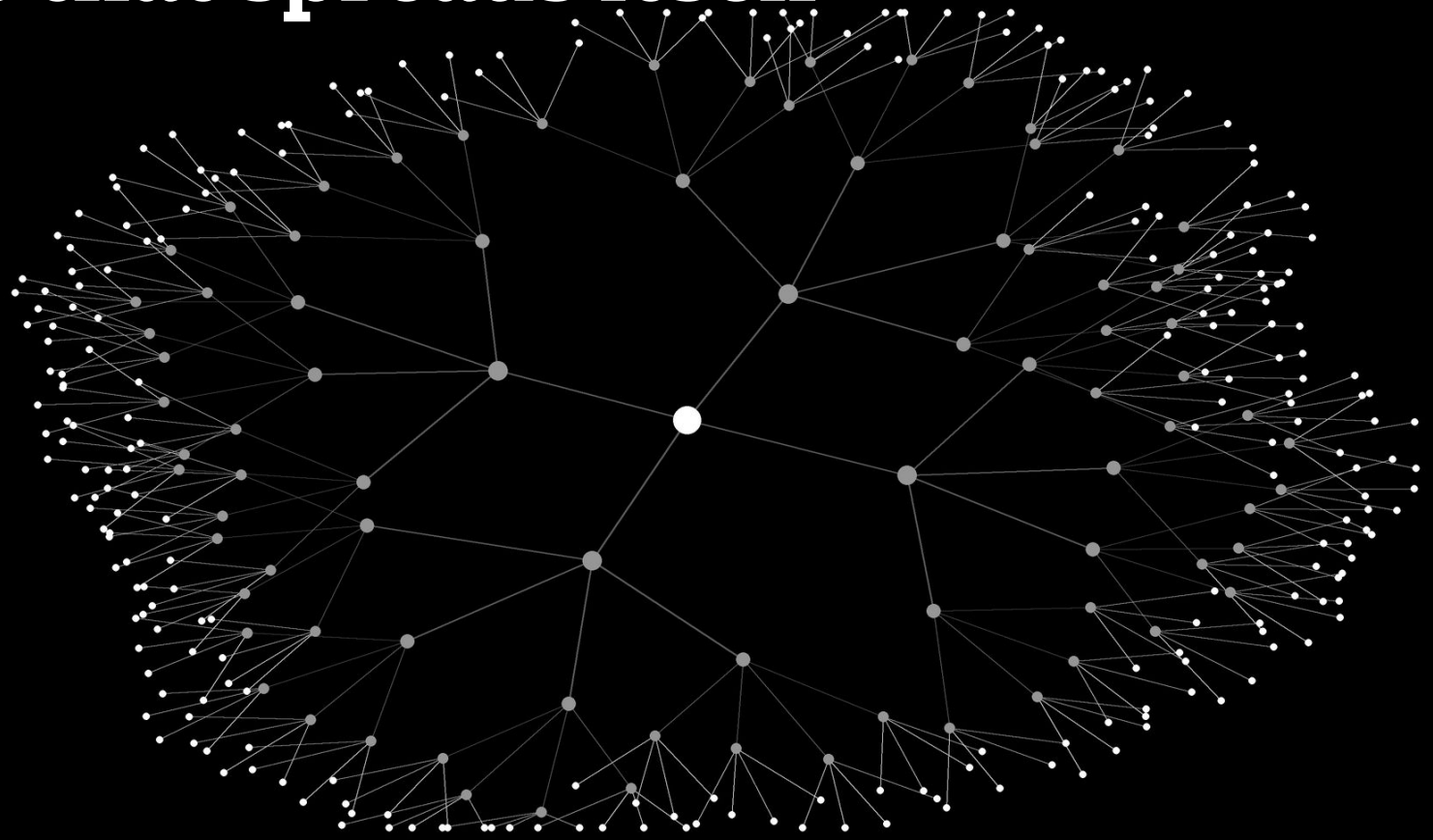


# The calendar invite that spreads itself

## 0 clicks

**73% of the companies we track were hit.**

*It lands on your calendar before you click anything.*



AegisAI

DETECTION

# It's AI vs. AI now. Your detection has to keep up.

01 · INBOX

### AI email security

Reads what a message asks for — a bank change, a payment, a login — and checks it against the real sender and thread history.

02 · PAYMENTS

### Fraud monitoring

Flags new payees, changed accounts and odd amounts. Use your bank's positive pay and payee checks.

03 · PEOPLE

### Verified process

Every change to where money goes is confirmed on a number already on file.

**THE POINT** · *people are the last line of defense, not the only one*

AegisAI

MONDAY MORNING

## This Week

01 Turn on Enhanced Safe Browsing

02 Create a database of trusted phone and account numbers you can proactively call to confirm

03 Write down the fraud plan: bank fraud line, then ic3.gov, same day.

## This Month

01 Turn on dual approval control - reduces urgency based attacks

02 Ensure your email and invoice systems can detect fraudulent emails

03 Audit device security for authorized approvers (secure device, network, and environment)

**Cy Khormaee**
cy@aegisai.ai · aegisai.com
linkedin.com/in/cykho

AegisAI

THANK YOU

# Curious what's reaching your team's inbox?

If it would help, we're glad to show your finance team what AI-written attacks look like in your own mail. No pitch — just the evidence.

**Cy Khormaee**
cy@aegisai.ai · aegisai.com

**QUESTIONS** · *find me after, or drop me a note*

Stifel's banking and lending services are provided by Stifel Bank, Member FDIC, and Stifel Bank & Trust, Member FDIC, Equal Housing Lender, NMLS# 375103 (collectively, "Stifel Banks"). Trust and fiduciary services are provided by Stifel Trust Company, N.A., Member FDIC, and Stifel Trust Company Delaware, N.A., Member FDIC (collectively, "Stifel Trust Companies"). Stifel Banks and Stifel Trust Companies are affiliated with Stifel, Nicolaus & Company, Incorporated, Member SIPC & NYSE, each a wholly owned subsidiary of Stifel Financial Corp. Unless otherwise specified, references to "Stifel" may mean Stifel, Nicolaus & Company, Incorporated or its affiliates.

Non-deposit products purchased from or held by Stifel, Stifel Banks, and/or Stifel Trust Companies are not insured by the FDIC, are not deposits, and may lose value. None of Stifel, Stifel Banks, or Stifel Trust Companies provide legal or tax advice.

AegisAI is not an affiliate of Stifel Bank.

Bank *with* STIFEL

**Stifel Bank** | One Financial Plaza | 501 North Broadway | St. Louis, Missouri 63102 | (866) 303-8003 | www.**bank**with**stifel**.com