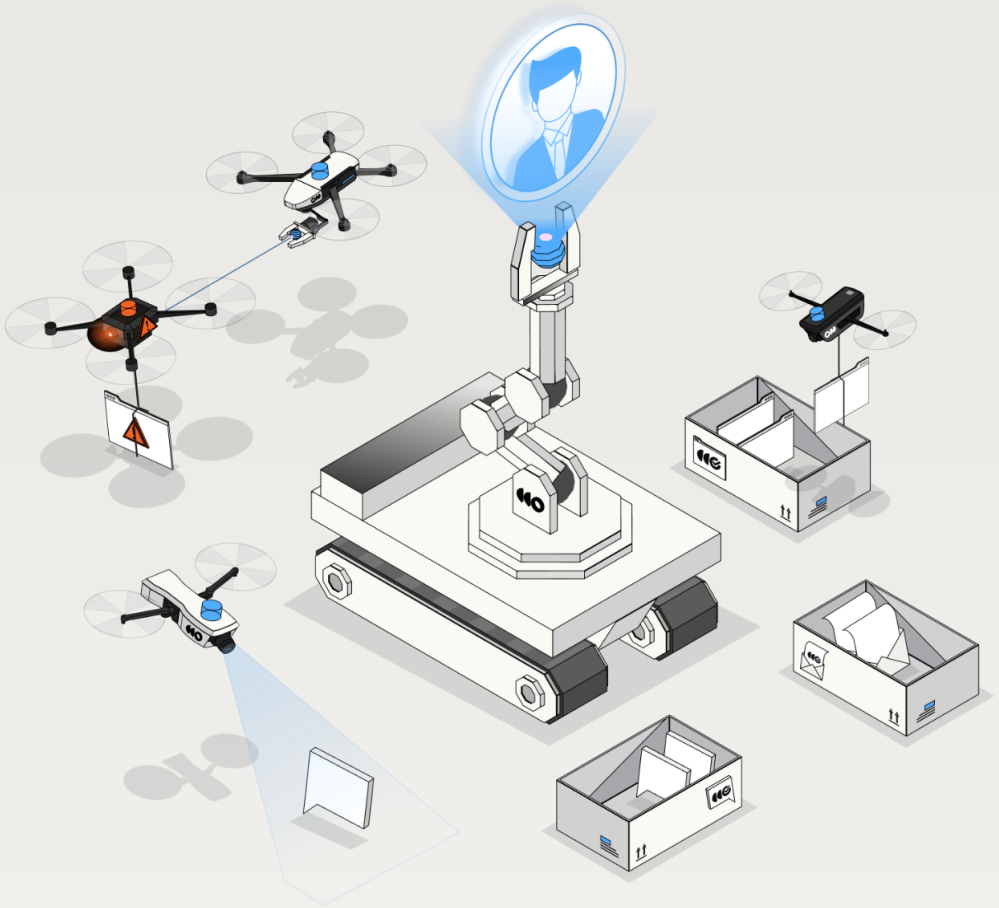
outtake

FIELD GUIDE 02

The Executive Impersonation Field Guide

Six attack patterns that use executive entities to commit fraud and put people at risk, and how to respond to each one.

A companion to the 2026 State of Executive Impersonation Report, drawn from 43,035 alerts across 270 monitored executives.



PURPOSE OF THIS GUIDE

Who this is for, and how to use it.

This is a field guide for CISOs, heads of security, and the people who have to decide what to do about executive impersonation. It names six real attack patterns, the signals that indicate each one, and a first action your team can take on each.

Goal of this guide

Most teams respond to executive impersonation one fake account or domain at a time. Removing a single fake rarely stops the person behind it from creating another.

This guide focuses on identifying who is behind an attack and removing the whole operation, not just the individual fake, before it leads to fraud, exposed data, or physical risk.

Where to start

Read the six patterns for where your program is most exposed. Use the self-assessment near the end to see where you stand today. Bring the board and leadership questions into your next planning conversation.

What this guide is not

It is not a longer takedown queue. Every pattern here is written to be traced back to an operator, not filed as an isolated incident.

It covers digital and physical risk together, because the same exposure feeds both. On the physical side that means the precursors: what an adversary can find about a person, and who is escalating toward them. It does not cover physical response, which stays with the protection team: travel risk, GSOC workflows, and protective intelligence operations.

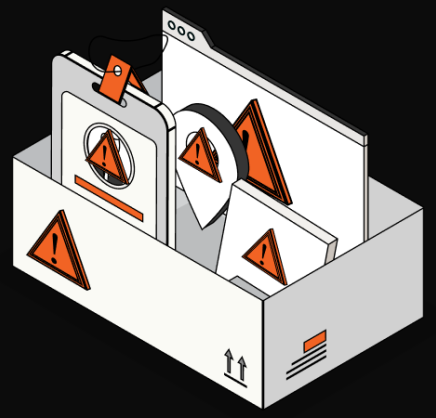
What it is built on

The 2026 State of Executive Impersonation Report: 43,035 alerts across 270 monitored executives.

THE PREMISE

"The fake you eventually see is a later stage of the attack, not the first one."

Outtake Labs, 2026 State of Executive Impersonation Report.



WHY THIS MATTERS NOW

How common this is.

The 2026 Digital Risk Report and the 2026 Digital Trust Industry Pain Report, both from Outtake, point to the same conclusion. Attackers are exploiting the trust people place in executives and employees, doing it across the open internet, and most security programs are not yet built to stop it.

84%

experienced material digital risk incidents in the past year

53%

had an executive or employee impersonated

77%

limit protection to executives, reactive cases, or a few high-risk roles

43%

have no person-of-interest threat profiling for targeted individuals

60%

of industries tracked name executive impersonation a primary or secondary pain point

Cybersecurity Insiders and Outtake, 2026 Digital Risk Report; Outtake Labs, 2026 Digital Trust Industry Pain Report.

This guide builds on a third report: the 2026 State of Executive Impersonation Report , Outtake's dedicated study of how executive impersonation shows up in practice, drawn from 43,035 alerts across 270 monitored executives.

What attackers are actually after.

Impersonating the executive is not the goal. It is the setup. The attacker borrows the executive's trust, then spends it on someone who can act. Two motivations drive almost all of it.

01

Financial gain

Move money. Approve a payment, change wire instructions, open access to funds. A bank robber with a better disguise.

02

Reputation destruction

Damage the person or the company. Fabricated statements, fake accounts, manufactured controversy, sometimes escalating into physical risk.

BY THE NUMBERS

$10.22M

average cost of a data breach in the United States, against $4.44M globally. Cheap for the attacker to create, expensive for the defender to remove.

IBM, Cost of a Data Breach Report, 2025.

Four paths to success

Once an executive is impersonated, the attacker picks a path. Each one ends somewhere the business feels it. This is the answer to the question a security team asks first: who cares if an executive gets impersonated on a social platform?

INTERNAL

A fake executive domain or email makes traditional phishing easy. Employees act because the request appears to come from the top.

PARTNER

Outreach to partners and investors asking for payment, documents, or a change to existing terms.

CUSTOMER

Scam ads, fake support, and fraudulent offers that spend customer trust in the brand until it runs out.

PUBLIC

Fabricated statements and manufactured controversy that become reputation damage, and in some cases physical risk.

Where this actually lives.

Executive protection has traditionally focused on physical safety. Cybersecurity has traditionally focused on the internal perimeter. A decade of security spending made the inside one of the best-defended places in business, so attackers went around it.

INTERNAL PERIMETER

What you defend

1. Endpoints
2. Identity
3. Email
4. Cloud

EXECUTIVE ENTITY

What they copy

1. Name
2. Face
3. Authority
4. Relationships

EXTERNAL PERIMETER

Where they use it

1. Ads
2. Domains
3. Messaging
4. Social
5. Events

Every pattern in this guide attacks the same thing: trust. Trust in your executives, in your brand, in the workflows that move money, and in the channels customers and employees use to reach you. That trust lives in public, on platforms you do not control. Most security programs were built to defend the internal perimeter. This sits outside it. That is the blind spot.

PEOPLE AS ATTACK SURFACE

Scope the program around who carries trust, not who holds a title.

Attackers do not stop at the executive suite. They go after whoever holds authority, access, relationships, or credibility. Board members, assistants, finance approvers, investor-facing leaders, customer-facing teams. Every one of them generates signals an attacker can study, copy, and use. A program scoped to senior titles misses most of the people being targeted.

35%

run no active PII removal program

52%

have no or limited visibility into encrypted channels

43%

have no person-of-interest threat profiling

96%

do not extend protection beyond a narrow set of executives

Outtake Labs, 2026 Digital Trust Industry Pain Report; Cybersecurity Insiders and Outtake, 2026 Digital Risk Report.

PII exposure is the seam, and it cuts both ways.

Credentials and account access on the digital side. Home address and family footprint on the physical side. The same broker listing or breach dump feeds both, so removing it once lowers both risks.

DIGITAL AND PHYSICAL

One executive. Two kinds of harm.

Executive protection is split into two programs with two buyers. The adversary does not respect that split: the same reconnaissance that precedes a wire fraud precedes a threat to a person.

EXECUTIVE DIGITAL RISK

What an adversary can copy. Who is spending your trust.

- Executive impersonation and likeness detection
- Cross-platform campaign detection
- Fraud and investment scams
- Negative chatter and narrative intelligence
- Email and password exposure
- Credential leaks and combolists

EXECUTIVE PHYSICAL RISK

What an adversary can find. Who is escalating.

- Home address exposure
- Physical location monitoring
- Person of interest monitoring
- Family and routine footprint
- Event and venue exposure
- Fixation and escalation signals

THE SEAM · PII EXPOSURE

One record. Two consequences.

A leaked credential is a digital problem. A leaked home address is a physical one. Both usually come from the same broker listing or breach dump. Remove it once and both risks fall.

Two programs, two buyers, one attack. The exposure that lets an adversary impersonate an executive is the same exposure that lets them find one.

THE DIGITAL TRUST KILL CHAIN

How an impersonation attack unfolds.

Eight stages across four zones. Zones 01 and 02 happen entirely on the open internet, before anything touches you. Five of the eight stages map cleanly to MITRE tactics. Trust exploitation has no dedicated tactic, target engagement only a partial one, and monetization sits outside MITRE's frame. Those gaps are the point.

ZONE 01 · DISCOVERY

Open internet · TA0043

01

Reconnaissance

Profiling the public surface: executive footprints, employee directories, event listings.

02

Infrastructure setup

Lookalike domains, fake executive accounts, ads, and email infrastructure get built.

AGENTIC SEARCH + ENTITY REGISTRY

ZONE 02 · EXPOSURE

Open internet · No MITRE tactic

03

Trust exploitation

The executive's name, face, and authority are borrowed to make new infrastructure look legitimate.

04

Target engagement

Bad actors launch the impersonating asset at customers, investors, and employees.

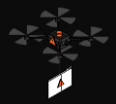
AGENTIC TRIAGE + NARRATIVE INTELLIGENCE

ZONE 03 · COMPROMISE

After contact · TA0001

05

Engagement capture



The target responds. A fake dashboard, an ongoing chat, a fake checkout.

06

Value transfer

The wire, the crypto payment, the counterfeit purchase. Account takeover is a minor branch.

AGENTIC RESPONSE + ADAPTIVE WORKFLOWS

ZONE 04 · HARM

After contact · Outside MITRE

07

Impact and fraud

Wire and transaction fraud, consumer scams, reputational damage, physical risk.

08

Monetization

Cashing out, credential resale, investor payout scams, money mules.

AGENTIC REFLECTION + DIGITAL TRUST RESERVOIR

CHEAPER TO STOP — COSTLIER TO ABSORB

Every stage is cheaper to disrupt than the one after it.

Most programs first detect at stage 04, once it reaches an inbox or an account. Zones 01 and 02 happen on the open internet, before anything touches the company.

Motive changes the tempo. When the goal is physical harm rather than money, the chain compresses: the adversary skips monetization and acts on what Discovery surfaced.

OUTTAKE LABS, DIGITAL TRUST KILL CHAIN.

OUTTAKE.AI · ©2026 OUTTAKE INC 08

Executive Scam Ads

PRIMARY SURFACE: PAID SOCIAL, MESSAGING APPS, FAKE LANDING PAGES
CUSTOMER FRAUD · INVESTOR FRAUD · BRAND TRUST

Attackers use an executive's name, face, or company affiliation in fraudulent ads to promote fake investment opportunities, exclusive access, crypto schemes, or private messaging groups.

How It Unfolds

The ad works because people recognize and trust the executive named or pictured in it. Variants launch in bursts, so removing one leaves the rest live, and new creative is redeployed within hours. Traffic routes off-platform within a step or two. What happens after that is Pattern 04.

Indicators To Watch

- Paid ads using executive names, faces, or company affiliation
- Multiple creative variants launched in a short window
- Ads driving users to WhatsApp, Telegram, or fake landing pages
- Variants resurfacing within hours of takedown, indicating automated redeployment

If This Is Missed

Customer fraud, investor loss, brand damage, executive escalation, and a takedown queue that keeps refilling faster than the team can work it.

FIRST ACTION FOR YOUR TEAM

Audit platform ad libraries, including Meta Ad Library and TikTok's Commercial Content Library, for executive-name and executive-likeness abuse. Track active scam ads as an ongoing security metric your team reviews regularly.

BY THE NUMBERS

400+

executive impersonations targeting Bill Ackman and Pershing Square eliminated by Outtake, found across 11,000+ scanned social profiles.

Outtake Digital Trust Reservoir, 2026.

OUTTAKE CAPABILITY

Threat Graphing and Narrative Intelligence map the accounts, pages, and domains behind a scam ad into one operation. For Meta ad takedowns, Outtake reports a 99.4% confirmation rate and 14.4-hour average takedown time.

Outtake platform performance data, 2026.

Fake Sites, Real Executives

PRIMARY SURFACE: LOOKALIKE DOMAINS, FAKE PORTALS, EMAIL INFRASTRUCTURE
BEC · CREDENTIAL THEFT · CUSTOMER DECEPTION

Attackers register domains that imitate the company, the executive office, investor relations, or an executive communications channel. Then they populate them with the executive's name, face, and title so the message that follows looks like it came from inside.

How It Unfolds

The domain creates false legitimacy for the message that follows. Registrations usually arrive in clusters, sharing a registrar, nameserver, certificate authority, or page template. A domain that looks parked today is often staged infrastructure waiting for a fundraising milestone, an earnings date, or an executive travel window.

Indicators To Watch

- Clustered registrations using executive, company, investor, or event naming
- Executive name, photo, bio, or signature appearing on a domain the company does not own
- Shared registrar, nameserver, certificate authority, or page templates
- Certificate issuance activity immediately preceding a campaign

If This Is Missed

Business email compromise, credential theft, fake portals, customer deception, and investor fraud.

FIRST ACTION FOR YOUR TEAM

Run a lookalike-domain audit against company names, executive names, investor terms, and event language. Separate parked domains from weaponized infrastructure and monitor both.

BY THE NUMBERS

50M+

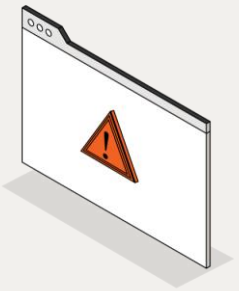
domains investigated by Outtake Agentic Search, with a mean takedown time of 3.5 days once a lookalike is confirmed.

Outtake Digital Trust Reservoir, 2026.

OUTTAKE CAPABILITY

Agentic Search separates parked lookalikes from weaponized infrastructure by clustering registrar, nameserver, and certificate signals, so staged domains surface before a campaign launches.

Outtake platform performance data, 2026.



PATTERN 03 · EXECUTIVE IMPERSONATION

Fake Investor and IR Communications

PRIMARY SURFACE: EARNINGS COMMUNICATIONS, INVESTOR UPDATES, PRESS STATEMENTS, IR DOMAINS
INVESTOR FRAUD · WIRE FRAUD · BOARD ESCALATION

Attackers impersonate executives or investor relations through fabricated earnings communications, quarterly updates, press statements, and distribution notices sent to shareholders, analysts, and internal finance teams.

BY THE NUMBERS

$2.77B

in reported business email compromise losses in 2024.

FBI IC3, 2024 Annual Report.

How It Unfolds

They exploit a calendar everyone already trusts. The message does not need to be unusual to work, it needs to arrive on schedule and look routine. Timing is the tell: IR-adjacent domains tend to appear just before an earnings date or a major announcement, when a payment instruction change draws the least scrutiny.

Indicators To Watch

- Payment or wire detail changes delivered inside an otherwise routine update
- Sender patterns mimicking the firm's real investor-relations format
- PDF metadata inconsistent with standard authoring tools
- IR-related domains registered ahead of earnings dates or announcements

OUTTAKE CAPABILITY

Threat Graphing connects a fake investor communication to the domains, accounts, and payment links behind it, identifying an average of 40+ connected nodes per campaign across 5+ platforms.

Outtake platform performance data, 2026.

If This Is Missed

Wire fraud, shareholder deception, material misinformation, confidential information loss, regulatory exposure, and board escalation.

FIRST ACTION FOR YOUR TEAM

Establish a canonical investor-communication channel and out-of-band verification for any change to wire instructions, capital-call details, or distribution notices.

PATTERN 04 · EXECUTIVE IMPERSONATION

Pig Butchering and Fake Platforms

PRIMARY SURFACE: MESSAGING GROUPS, FAKE TRADING PLATFORMS, DEEPFAKE VIDEO, APP STORES
CUSTOMER FRAUD · BRAND ASSOCIATION · EXECUTIVE REPUTATION

Attackers borrow an executive's name, face, and credibility to front fabricated investment platforms, then run a long con on the public. The company is not the victim. The company is the credential.

BY THE NUMBERS

$6.57B

lost by victims to investment fraud in 2024, the largest single IC3 cybercrime category.

FBI IC3, 2024 Annual Report.

How It Unfolds

This one does not start with an email. It starts with an ad and a private chat. What follows is a relationship, not a request: weeks of contact, a working dashboard, small withdrawals that clear. Then a larger deposit, and the platform goes dark. Victims report it to the company, not the platform.

Indicators To Watch

- Branded messaging groups on Telegram, WhatsApp, or Signal
- Synthetic video or voice endorsing a trading platform, fund, or token
- App listings and domains pairing an executive name with invest or trading
- Inbound support or legal contacts from people who were never customers

OUTTAKE CAPABILITY

Likeness matching finds the executive's face and voice in ads and video where text monitoring finds nothing, then links each placement to the payment rails behind it. [ADD METRIC]

Outtake platform performance data, 2026.

If This Is Missed

Customer and public financial loss, support and legal intake load, platform and regulator escalation, executive reputation damage, and durable association of the brand with fraud.

FIRST ACTION FOR YOUR TEAM

Search paid ad libraries and messaging platforms for your executives' names paired with investment language. Confirm you have a takedown path with each platform before you need one.

Fake Hiring Outreach

PRIMARY SURFACE: LINKEDIN, X, TELEGRAM, WHATSAPP, EMAIL, JOB BOARDS
CREDENTIAL THEFT · CANDIDATE FRAUD · BRAND DAMAGE

Attackers impersonate executives, recruiters, or hiring teams to target candidates, employees, contractors, or partners.

How It Unfolds

Hiring creates a trusted reason for strangers to exchange information. A candidate expects to hand over identity documents, banking details, and personal history early, and expects the conversation to move to a personal channel. That expectation is the attack surface. The company usually learns about it from the candidate, after the fact.

Indicators To Watch

- New recruiter profiles using company or executive branding
- Job postings not present in the official applicant tracking system
- Candidate outreach routing to unofficial domains or messaging apps
- Requests for identity documents or payment details before a formal offer

If This Is Missed

Credential harvesting, candidate fraud, employee compromise, brand damage, and legal escalation.

FIRST ACTION FOR YOUR TEAM

Publish and reinforce a canonical careers URL. Treat any hiring communication outside that domain or the official applicant tracking system as suspicious until verified.

BY THE NUMBERS

$750.6M

in reported business and job opportunity fraud losses in 2024.

FTC, Consumer Sentinel Network 2024 Data Book.

OUTTAKE CAPABILITY

Recon Agent researches a suspected fake recruiter 38 times faster than manual review, an average of 16 minutes against 5.6 hours. 40% of Recon Agent reports surface actor identity leads.

Outtake platform performance data, 2026.

Family and Inner-Circle Exposure

PRIMARY SURFACE: PUBLIC RECORDS, SOCIAL, SHORT-FORM VIDEO, CHARITY PAGES, MESSAGING APPS
DONATION AND INVESTMENT FRAUD · DOXXING · PHYSICAL ESCALATION

Attackers target the people around an executive: family, assistants, household staff, and board contacts. Then they impersonate them, because a spouse carries the executive's trust with none of the scrutiny.

How It Unfolds

Most programs define "executive" narrowly. Attackers do not. Adjacent identities are public by default, which makes them the cheaper disguise. A fake spouse account on short-form video soliciting charitable donations, routed to a private chat, is the same fraud as a fake executive account. It just draws less scrutiny.

Indicators To Watch

- Replicated family, assistant, or household-adjacent profiles
- Doxxed home addresses or personal details tied to family members
- Repeat actors returning to the same executive across platforms, a fixation signal
- Family or assistant accounts soliciting donations, investments, or payments

If This Is Missed

Donation and investment fraud run under a family member's name, doxxing, stalking, harassment, extortion, and physical safety escalation.

FIRST ACTION FOR YOUR TEAM

Expand protection scope to immediate family and high-risk adjacent identities. Document what is public, what can be removed, and who may ever solicit money in the executive's name.

BY THE NUMBERS

41

impersonations found across one executive and their family members in a single financial services engagement: 28 of the executive, 13 of relatives.

Outtake Recon Agent, anonymized customer findings.

OUTTAKE CAPABILITY

Agentic Search extends coverage to a full Person of Interest dossier across family and household-adjacent identities, detecting in about 15 minutes against a 7 to 9 hour manual baseline.

Outtake platform performance data, 2026.

WHY THE ARTIFACT IS NEVER THE TARGET

One likeness. Nine surfaces. One app.

Recon Agent followed a single impersonated executive across social profiles, paid ads, messaging accounts, and lookalike sites. Nine confirmed surfaces, all funnelling into the same fake mobile app collecting deposits.

THE SOURCE

One executive's likeness

Name, face, and title lifted from public material. Nothing was breached to get it.

NINE CONFIRMED SURFACES

- Social profiles
- Paid ads
- Messaging accounts
- Lookalike sites

THE LEVERAGE

One fake mobile app

Every surface routes here. One backend, one hosting account, shared with roughly seven sibling clones.

Take down one surface and the app keeps collecting.

9

impersonation surfaces mapped from one signal

1

fake mobile app collecting the deposits

~7

sibling clones sharing the same portal fingerprint

2.5yr

of campaign history on record

OUTTAKE RECON AGENT. ANONYMIZED FINDINGS FROM A FINANCIAL SERVICES CUSTOMER.

This is the difference between a takedown queue and a program. Nine tickets closed one at a time leaves the app running. One investigation that reaches the backend ends the campaign.

A NEW APPROACH · NEXT-GENERATION DRP

The Digital Trust Funnel.

Outtake is a Next-Generation Digital Risk Protection platform. It runs five stages as one loop: you set the objective and the policy, the agents do the work, and everything is visible in-platform and available over API and MCP.

EVERYTHING PUBLIC ABOUT YOUR ENTITIES

CONFIRMED THREATS, REMOVED

01

Agentic Search

Multi-platform and multimodal. Know the footprint before you defend it.

ENTITY REGISTRY

02

Data Enrichment

Semantic search and entity detection cut the noise. No keyword lists.

SIGNALS

03

Investigation

Connect actors, infrastructure, and author tracing. The network, not the asset.

THREAT GRAPHING AND NARRATIVE INTELLIGENCE

04

Action

Remove and report at machine speed, inside your approval controls.

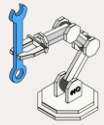
ADAPTIVE WORKFLOWS

05

Measure and Adapt

Every action feeds back into detection, so the system compounds.

DIGITAL TRUST RESERVOIR



EVERY ACTION SHARPENS THE FUNNEL

DEFINITION

Next-Generation Digital Risk Protection (NGDRP)

Technology that continuously discovers, investigates, and remediates the impersonation, fraud, and coordinated threats targeting a company's brand, executives, locations, and products across the open internet. It advances earlier DRP by running the full detection-to-response cycle autonomously and at machine speed, acting on the operation behind an attack rather than the individual fake, and improving with each case under your policies and approvals.

SELF-ASSESSMENT

Maturity levels for your program.

Mark where your program sits at each stage of the kill chain, then start with whichever stage is weakest. Tier 3 is what Outtake calls Next-Generation DRP in practice: agents working continuously across detection, investigation, and takedown, where each case improves the next.

KILL CHAIN STAGE	TIER 1: REACTIVE	TIER 2: MANAGED	TIER 3: ADAPTIVE
Reconnaissance	No POI profiling. Exposure unaddressed.	POI for executives. Broker removal periodic.	Continuous automated monitoring across executives and the broader workforce.
Infrastructure Setup	No watch for lookalike domains or fake accounts.	Periodic scans. Partial detection. Reactive cleanup.	Continuous detection across domains, accounts, and bot networks, so new infrastructure is found as it appears.
Trust Exploitation and Target Engagement	Detection arrives from customers or external reports.	Active monitoring with gaps. Some campaign mapping.	One signal is enough to spot related activity across channels and identify who is behind it.
Impact, Fraud and Monetization	Manual takedown. Ad hoc response.	Standardized takedown with partial measurement.	Removing the attacker's network, not one account. Each case improves detection for the next.

BOARD AND LEADERSHIP QUESTIONS

Questions worth asking out loud.

- Who owns executive impersonation risk across security, fraud, legal, communications, investor relations, and executive protection?
- Where do we first detect it today: our own controls, a customer, a partner, the executive, or after public harm?
- Can we see impersonation across social, domains, ads, messaging apps, open web, dark web, and event surfaces?
- Can we connect a fake account, spoofed domain, scam ad, messaging channel, and payment link back to the same operator?
- What is our takedown SLA by channel, and where do these threats persist longest?
- Do we protect only executives, or also assistants, board members, finance approvers, family members, and public-facing employees?
- Are we measuring takedowns completed, or whether the underlying operation was removed?

If the program cannot run detection, investigation, takedown, and verification as one connected process, it is not a program. It is a case queue.

CISO AND CSO CHECKLIST

Use this as the working session agenda.

01 **Scope**

List protected executives, board members, spokespeople, family adjacencies, assistants, and investor-facing leaders.

02 **Surfaces**

Document coverage across social, domains, ads, messaging, dark web, forums, and geo.

03 **Workflows**

Define verification for wires, investor communications, recruiting outreach, and payment changes.

04 **Signals**

Identify where the first signal is expected to appear and who receives it.

05 **Response**

Measure takedown SLA by channel and track whether the operator was removed.

06 **Briefing**

Create an evidence-grade executive risk briefing for security, GSOC, legal, comms, and leadership.

WHAT TO DO NOW

Five steps to take.

These five steps work best as one connected process. Done separately, they turn into a series of one-off cleanups instead of a program.

01

Cut personal exposure

Profile who attackers map first: executives, high-risk roles, family, and assistants. Remove exposed PII.

02

Find campaign infrastructure early

Discover lookalike domains, fake accounts, and scam ads continuously. Attribute each one to its operator.

03

Cover every channel

Cover email, social, mobile, encrypted messaging, app stores, marketplaces, and dark web.

04

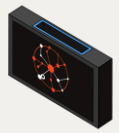
Verify high-value workflows

Monitor credentials continuously. Require out-of-band verification for wires and payment changes.

05

Look past the takedown

Removing a fake is one step. Trace who is behind it and use what you learn on the next case.



Outtake runs detection, investigation, takedown, and verification as one continuous loop, at machine speed.

See how Outtake protects the people who represent your brand.

Across every platform, every entity, in real time.

Book a Demo →

SOURCES & CITATIONS

Public data, public sources.

Public statistics and incident references are sourced from the materials below. Proprietary figures, including the Outtake capability notes on each pattern page, are drawn from the Outtake Digital Trust Reservoir and platform performance data, and are labeled as such.

PRIMARY RESEARCH

01 Cybersecurity Insiders and Outtake, 2026 Digital Risk Report, survey of 1,138 security, fraud, digital risk, and trust leaders.

02 Outtake Labs, 2026 Digital Trust Industry Pain Report.

03 Outtake Labs, 2026 State of Executive Impersonation Report (n=43,035 alerts across 270 executives, Outtake Digital Trust Reservoir).

04 Outtake platform performance data and customer engagement results, 2026.

05 Outtake market analysis, 2026.

06 Outtake Labs, The Digital Trust Kill Chain, go.outtake.ai/labs/digital-trust-kill-chain.

PUBLIC DATA AND REPORTING

06 FBI Internet Crime Complaint Center, 2024 Annual Report.

07 Federal Trade Commission, Consumer Sentinel Network 2024 Data Book.

08 IBM, Cost of a Data Breach Report, 2025.

09 Privacy Rights Clearinghouse, 2025.

10 Identity Theft Resource Center, 2025 Annual Data Breach Report.

11 UnitedHealth Group, 2025 Proxy Statement.

12 OECD AI Incidents Monitor.

13 U.S. Department of Justice public filings related to impersonation and recruiting fraud.