Doppel



# Why Financial Institutions Choose Doppel

Defending against modern social engineering attacks.

## A New Risk Reality

Financial institutions are facing a fundamental shift: social engineering is now the primary driver of fraud, account takeover, and customer loss.

Attackers are targeting the weakest link in the system — trusted interactions between customers, employees, advisors, and contact centers. And they're using AI to execute with more precision and scale than ever before.

Doppel exposes risks and eliminates threats across every digital channel, before these attacks impact your customers, brand, people, or revenue.

## Key Threats Facing Financial Institutions

### Executive & Advisor Impersonation

Targeting wealth advisors, brokers, and executives to initiate high-value transfers or manipulate clients and contact centers.

### Contact Center & Vishing Attacks

Exploiting call center workflows and identity verification gaps to bypass controls.

### Credential Theft & Account Takeover

Phishing, fake apps, and spoofed login flows leading to account compromise.

### Brand Abuse Across Digital Channels

Fraudulent investment ads, spoofed domains, and fake banking apps targeting customers.

### Data Exposure

Leaked PII and credentials fueling downstream financial fraud and identity abuse.

# Doppel for Financial Services: A Unified Defense Platform

Legacy security and fraud tools are effective against technical threats, but fail when AI-driven social engineering manipulates users to bypass controls.

Attackers operate in coordinated campaigns across voice, domains, social, and messaging, while traditional solutions remain siloed, reactive, and blind to how these threats actually connect.

Doppel unifies detection, intelligence, response, and resilience into a single platform, extending into targeted training and real-world simulation, so financial institutions can continuously adjust to and defeat the modern threats they're actually facing.

## Security Awareness Training

Traditional awareness programs fail because they're static and disconnected from real threats.

Doppel delivers targeted, role-specific training built from actual attack activity targeting your institution:

- **Deepfake-driven, custom content featuring your executives and brand, and built for your policies and workflows**
- **Automated training flows for onboarding and continuous reinforcement**
- **Personalized, interactive coaching with real-time feedback to drive behavior change**

Doppel transforms awareness into measurable behavior change by aligning training directly to real attack tactics and financial workflows. This increases employee vigilance against sophisticated social engineering attacks, focuses remediation where it matters most, and ensures teams can recognize and stop fraud before damage occurs.

## Simulation

Doppel simulates live attack scenarios across channels to identify breakdowns before attackers exploit them:

- **Multi-channel simulations across phishing, vishing, and messaging attacks**
- **Threat-informed campaigns based on real attacker tactics and infrastructure**
- **Agentic AI-driven flows that create dynamic, personalized attack scenarios in minutes**

Doppel gives financial institutions a safe environment to test and validate their defenses against real attacker tactics. By exposing gaps in identity verification, escalation, and response processes, institutions can continuously improve resilience, reduce fraud risk, and demonstrate readiness against revolving regulatory expectations.

## Brand Protection

Doppel autonomously detects and dismantles impersonation and fraud targeting your institution across:

- Lookalike banking domains and spoofed login portals
- Fraudulent mobile apps and investment platforms
- Social media impersonation and messaging scams
- Paid ads driving traffic to malicious destinations

Doppel shuts down fraudulent experiences before customers ever interact with them, reducing unauthorized transactions, account takeover, and scam-driven losses. By eliminating impersonation at the source, financial institutions protect digital channels, preserve customer trust, and prevent fraud from scaling into systemic risk.

## Executive Protection

Executives, advisors, and relationship managers are prime targets for high-impact fraud.

Doppel protects both executives and customers from:

- AI-generated impersonation and deepfake-enabled fraud
- Targeted vishing attacks against executives and client-facing teams
- Exposure of sensitive personal and professional data used in social engineering

Doppel reduces the risk of fraudulent wire transfers, client manipulation, and high-value social engineering attacks targeting leadership and advisors. This is critical for protecting high-net-worth client relationships, maintaining fiduciary trust, and minimizing regulatory and reputational fallout tied to executive compromise.

## Threat Graph Intelligence

Doppel connects signals across domains, voice, social, email, telco, and more to uncover coordinated attack campaigns targeting your institution, and provides actionable context to make strategic decisions.

Threat Graph Insights:

- Map coordinated fraud campaigns end-to-end linking phishing domains, fake apps, impersonation, and attacker infrastructure into investigation-ready views

Threat Intelligence Reports:

- Analyst-led deep-dives that map attacker tactics, infrastructure, and reuse patterns, translating threat activity into clear financial, operational, and regulatory risk with remediation guidance

Executive Strategy Briefings:

- Portfolio-level visibility and senior-ready narratives that connect threats to business impact, equipping executives with clear priorities, risk alignment, and actionable remediation roadmaps across brands and subsidiaries

ARK INVEST

**How Doppel Protects Ark Invest**

ARK Invest, a leading investment management firm with a high-profile digital presence, faced growing risk from impersonation and social engineering attacks targeting its brand and investors. These attacks were spreading rapidly across platforms like LinkedIn, Instagram, WhatsApp, and Telegram, creating real exposure to fraud, reputational damage, and operational disruption.

By partnering with Doppel, ARK moved from manual, reactive “whack-a-mole” defenses to automated, AI-driven detection and takedown across social media, domains, and the dark web, stopping coordinated campaigns before they could scale.

- 98% takedown success rate
- 5.5 hours: median domain resolution time
- 10,500+ verified alerts

# Regulation and Compliance Readiness

## Vishing is now a regulatory priority

Financial regulators are no longer treating social engineering as a theoretical risk; they’re codifying it into enforceable requirements.

Recent updates (including NYDFS guidance) explicitly call for targeted awareness training that addresses real-world vishing and impersonation attacks, not generic, one-size fits all programs.

## The Compliance Gap

Most financial institutions struggle to meet these expectations because training is generic and not tailored to high-risk roles like contact centers or advisors, employees are not tested against realistic vishing scenarios, critical workflows like identity verification and call center escalation are never pressure-tested, and there’s no measurable way to track human risk over time.

This gap leaves institutions exposed to both fraud losses and regulatory scrutiny, especially as examiners increasingly evaluate real-world readiness.

## How Doppel Enables Compliance and Reduces Risk

Doppel operationalizes what regulators are asking for: Targeted, threat-informed, and continuously validated human risk programs.

### Vishing & Social Engineering Simulation

- Simulate real attacker behavior across voice and digital channels
- Test identity verification, escalation, and response processes
- Identify breakdowns in high-risk workflows

Executives, advisors, and relationship managers are prime targets for high-impact fraud.

### Targeted Awareness Training

- Role-specific training tailored to contact center agents, advisors, and executives
- Focused on vishing, impersonation, and financial fraud scenarios
- Continuously updated based on active threats targeting your institution

### Human Risk Measurement

- Quantify susceptibility across roles, teams, and business units
- Track improvement over time with defensible metrics
- Provide evidence for audits, regulators, and internal stakeholders

### Threat-Informed Strategy

- Use real Doppel threat intelligence to shape training and simulations
- Align programs directly with NYDFS targeted awareness requirements and frameworks like MITRE ATT&CK and NIST

## From Compliance Burden to Security Advantage

With Doppel, financial institutions can move beyond checkbox compliance to demonstrable resilience

- Prove readiness against vishing and social engineering attacks
- Strengthen compliance posture across NYDFS, FFIEC, GLBA, FINRA, DORA, and NIS2
- Reduce fraud driven by human error and process gaps
- Build a defensible, audit-ready human risk management program

## The Bottom Line

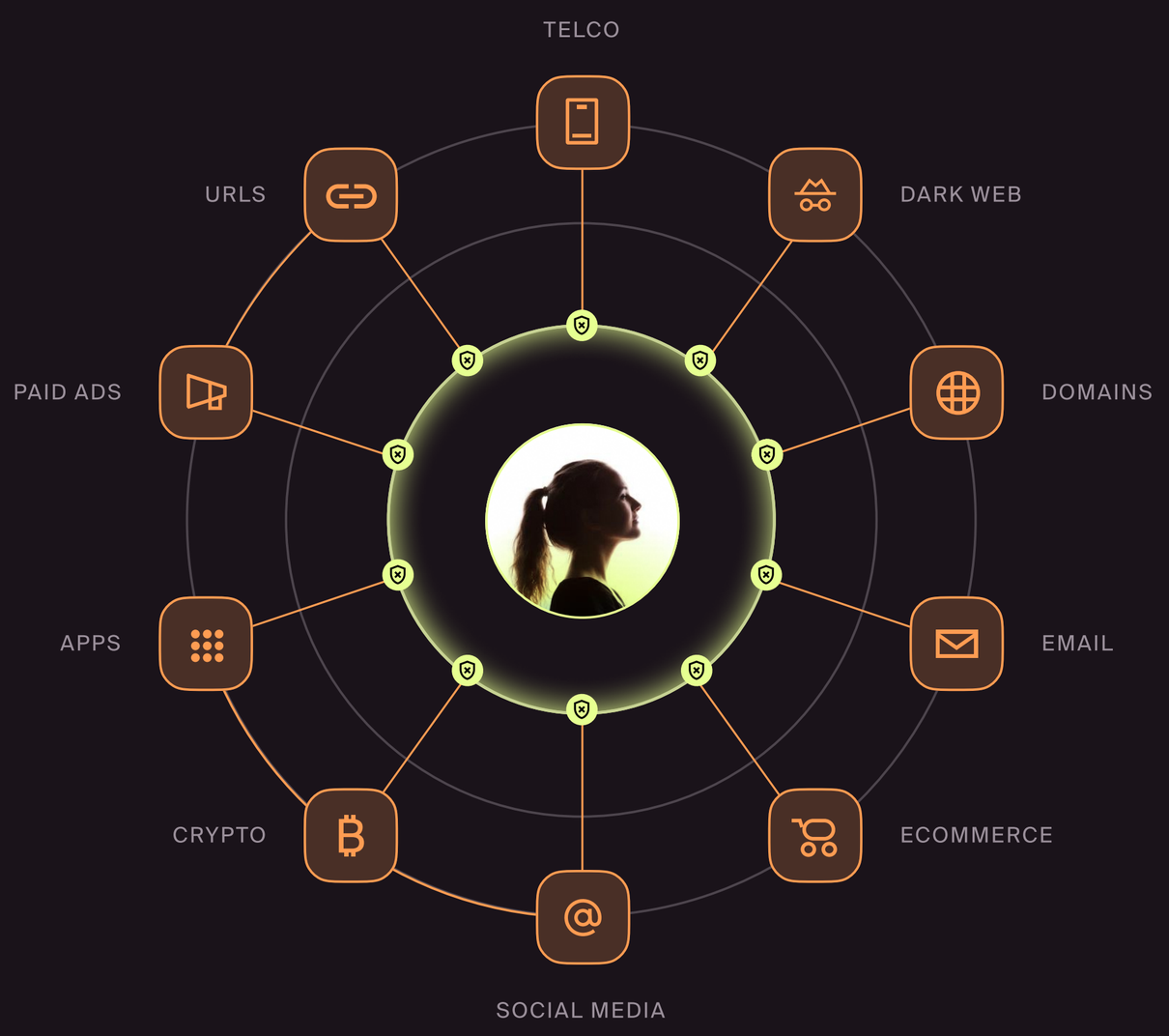
Regulators are making one thing clear: human risk is now a first-class control surface.

Doppel gives financial institutions the ability to see social engineering attacks clearly, stop them early, and prove their ready for what's next.

### AI-Driven threat mapping, validation and disruption

Doppel protects people and brands from AI-powered impersonation, fraud, and social engineering. We don't just detect threats, we dismantle the attacker's infrastructure across every channel it touches.

- **Multi-channel signal ingestion**
- **Cross-surface correlation into unified threat graph**
- **Automated enforcement across registrars, telcos, ad networks, platforms**
- **Feedback loop → threat graph learns from every takedown**




Book your demo at doppel.com/request-a-demo