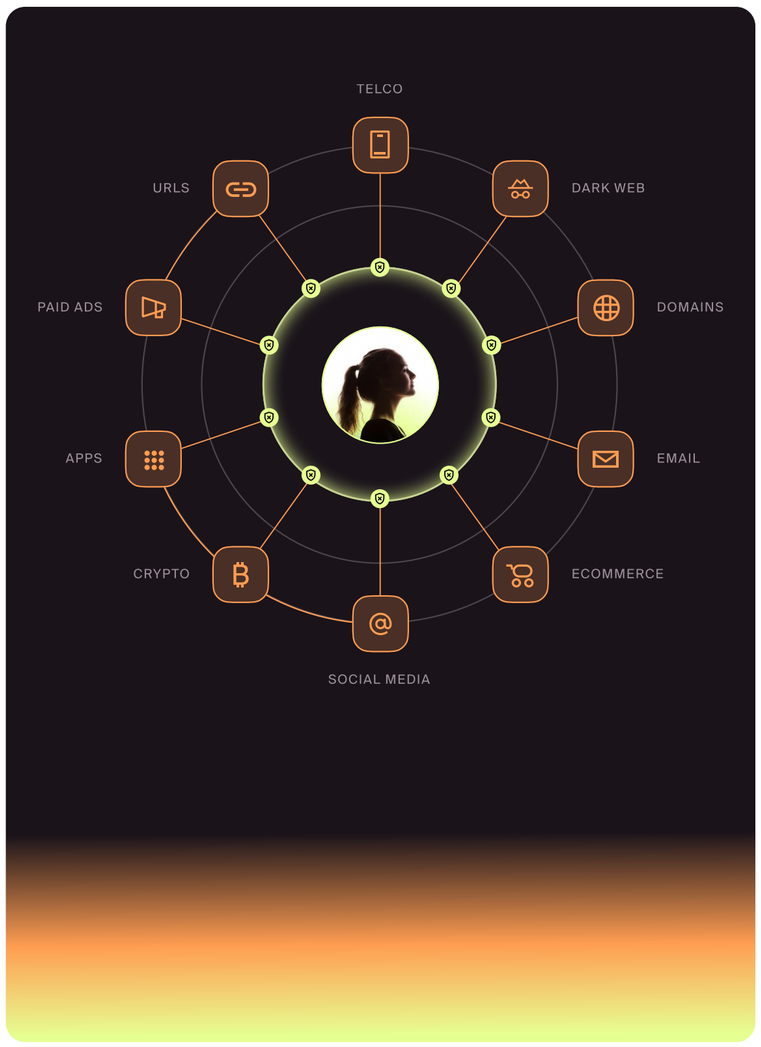
FINANCIAL SERVICES

Doppel

Social Engineering in Financial Services

Protecting your brand, customers, employees, and revenue from AI-driven fraud & scams

The growing attack surface



In financial services, trust is the foundation of every customer relationship. It's also the primary target for attackers.

As institutions expand across digital channels, the attack surface grows with them. Threat actors are exploiting this shift with sophisticated impersonation and social engineering attacks targeting both customers and employees.

These attacks are no longer isolated. They are coordinated, persistent, and built to scale, spanning domains, social media, paid ads, messaging platforms, app stores, and voice.

Using AI-generated content, deepfakes, and spoofed identities, attackers create highly convincing interactions that exploit trust at speed. What once took weeks now takes minutes.

External threats do not stay external. They lead to:

- Customer scams and unauthorized transactions
- Account takeover and credential compromise
- Loss of customer trust and brand damage
- Increased fraud losses
- Regulatory scrutiny and compliance risk

Threats to Financial Institutions

- **Executive & Broker Impersonation:** AI-generated messages, deepfakes, and vishing are used to convincingly impersonate executives and advisors, manipulating trust to initiate high-value transactions and fraud.
- **Phishing & Credential Theft:** Lookalike domains, fraudulent contact center interactions, fake banking apps, and coordinated phishing campaigns capture customer credentials and enable account takeover within seconds.
- **Rising Regulatory Risk:** Regulators are increasingly focused on real-world attack scenarios, including vishing. This drives greater emphasis on training, testing, and simulation aligned to frameworks such as NYDFS, NIST, and MITRE ATT&CK.
- **Brand Abuse Across Channels:** Fake ads, spoofed websites, and brand impersonation across social and messaging platforms exploit trust to deceive customers at scale and drive fraudulent engagement.
- **Data Exposure:** Leaked PII, payment data, and credentials circulate across the open web, fueling downstream fraud and compounding both security and reputational risk.

$4.6B+
Losses from Investment scams which leads all fraud categories
SOURCE: FTC

98%
of cyberattacks involve Social Engineering
SOURCE: SPLUNK

30.9%
of all phishing attacks target payment platforms and financial institutions
SOURCE: APWG REPORT Q1 2025

60 SECS
median time to submit credentials in which users fall for phishing
SOURCE: VERIZON DBIR 2024

FINANCIAL SERVICES

Doppel

Where Existing Tools Fall Short

Most financial institutions already have multiple tools in place, but those tools were not designed for modern attack patterns. Visibility is fragmented across fraud, security, brand, and threat intelligence teams, leaving each with only a part of the picture. Analysts are forced to manually stitch together signals across channels, while high alert volume creates noise that obscures real threats. When threats are detected, response is often slow or ineffective.

Modern Threats Require Modern Solutions

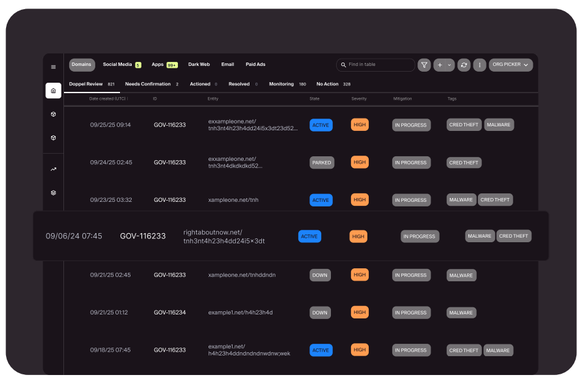
Doppel defends against the full social engineering attack surface by unifying detection, correlation, and disruption across domains, social, messaging, voice, paid ads, and more. It identifies and prioritizes high-risk threats tied to impersonations, fraud, credential theft, and data exposure, cuts through alert noise, and automates takedowns of malicious infrastructure before it can scale. By connecting signals across channels, Doppel provides a single, actionable view of coordinated attack campaigns, giving teams the context needed to prioritize and respond effectively.

Doppel also strengthens internal resilience by simulating real-world attacks, testing helpdesk and contact center workflows, and delivering targeted, role-specific training. This helps organizations identify gaps in identity verification, reduce human risk, and align with evolving regulatory expectations.

With Doppel, financial institutions move from reactive response to proactive risk reduction:

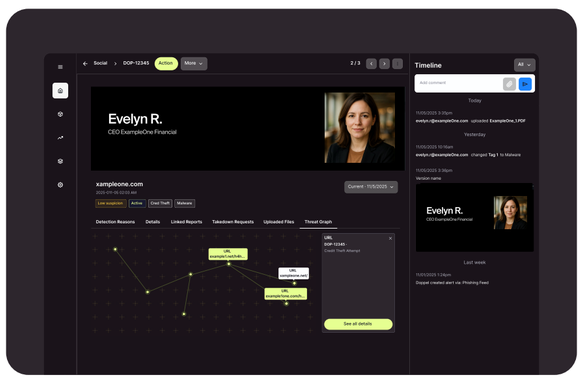
- Stop scams and account takeover before they impact customers or funds
- Protect customer trust and brand reputation from impersonation and abuse
- Reduce fraud risk driven by credential theft, data exposure, and social engineering
- Accelerate detection and disruption of threats across all digital channels
- Cut through alert noise and reduce manual investigation
- Strengthen compliance readiness across PCI DSS, FFIEC, NYDFS, GLBA, and FINRA
- Simulate real-world attacks and pressure-test employees, helpdesk, and executive workflows
- Identify and close gaps in identity verification and response processes
- Measure human risk and deliver targeted training

Solutions powered by the Doppel Platform



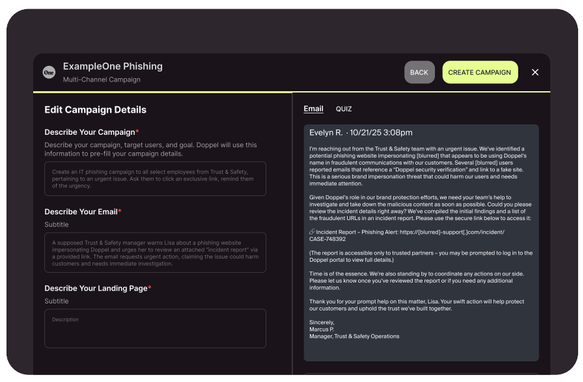
Brand Protection

Detect and remove impersonation, brand abuse, and fraud across domains, apps, social media, messaging platforms, and more.



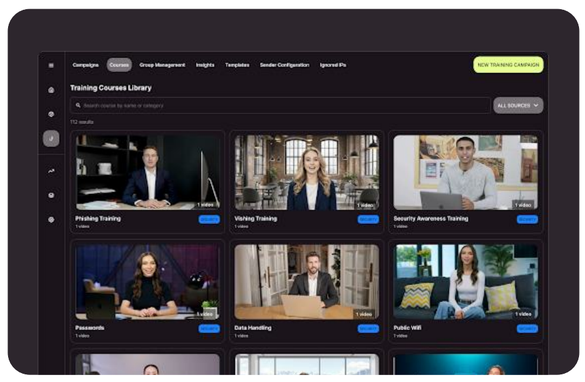
Executive Protection

Protect executives from impersonation, targeted social engineering, and sensitive data exposure.



Simulation

Test employees, executives, and contact centers against real-world attack scenarios across channels.



Security Awareness Training

Train employees to recognize and respond to modern social engineering tactics. Financial institutions can no longer rely on siloed tools to defend against coordinated, multi-channel social engineering attacks.

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