WILLKIE

CLIENT ALERT

Vishing – The New Phishing: Different Tactics, Same Strategic Goals

August 17, 2026

AUTHORS

Daniel K. Alvarez | Laura E. Jehl | Briony Pollard | Alexandra Barczak

The threat environment facing financial institutions and their service providers continues to evolve rapidly. Over the past month, sophisticated and coordinated cyber campaigns have targeted the financial services sector, including some of the most prominent institutions on Wall Street. As reported by various news sources, such as the Financial Times, in early August 2026, ransom-seeking threat actors launched attacks against a number of major U.S. financial institutions, private equity firms, hedge funds, and related professional services organizations that collectively manage hundreds of billions of dollars and maintain complex systems containing highly sensitive trading, client, and investor data. Financial services firms remain prime targets for financially motivated threat actors because they hold highly sensitive data—the unauthorized disclosure of which would likely trigger regulatory reporting obligations, contractual notification requirements, litigation exposure, and reputational harm on a scale that few other industries face—and are financially able to make large payments in an effort to prevent the disclosure of that data.

These latest campaigns represent an escalation in both targeting precision and tactical sophistication. The threat actors employed effective social engineering strategies, relying primarily on voice phishing ("vishing") to compromise targets. In vishing incidents, attackers contact employees on their personal cellphones, not just office

lines, and impersonate an organization's internal help desk, in some instances displaying the correct help desk phone number through caller ID spoofing. They claim urgent IT directives requiring employees to update passkeys or MFA credentials, then direct victims to convincingly spoofed websites. When employees enter their credentials on these fraudulent sites, the attackers harvest passcodes live over the phone and hijack accounts within seconds. AI tools are enabling attackers to scale these campaigns more cheaply and broadly, using voice mimicry technology to impersonate trusted persons with increasing fidelity. These methods are designed to manipulate human trust, circumvent technical controls (bypassing email-based security filters entirely) and exploit the reality that even well-trained employees may not expect a social engineering attack delivered by voice. Accordingly, such attacks are particularly dangerous for organizations that have not specifically trained personnel to recognize them.

In light of this active threat landscape, financial institutions and other organizations handling sensitive data should consider taking proactive steps now, before an incident occurs, to review and strengthen their defensive posture.

1. *Update Cybersecurity Training*: Cybersecurity awareness training programs should be promptly updated to address the latest threat actor tactics and social engineering methods identified in recent incidents, including vishing, help-desk impersonation, MFA and passkey-reset lures, personal-phone targeting, AI-enabled voice mimicry, and spoofed support websites. All personnel within the organization should complete updated training modules as soon as feasible, the content of which should be regularly pressure-tested to ensure that it addresses the latest threat intelligence.

2. *Update Incident Response (IR) and Disaster Recovery (DR) Policies*: IR and DR plans should be updated to ensure that they are current, actionable, and appropriately tailored to vishing and account-takeover scenarios. This process should confirm that IR/DR plans include up-to-date contact information for critical stakeholders, including internal decision-makers, outside counsel, forensic investigation vendors, cyber insurance carriers, relevant regulators, communications and public relations advisers, law enforcement contacts, and critical technology vendors. Plans should clearly define escalation protocols, decision-making authority, and communication procedures for scenarios involving compromised credentials, unauthorized system access, potential data exfiltration, and ransomware demands. Organizations that have not reviewed their IR/DR documentation within the past six months should treat this as a priority.

3. *Review Legal Notification, Privilege, and Exposure Workflows*: In conjunction with number (2) above, breach notification and escalation workflows should be reviewed and updated to ensure that events identified in press reports are promptly routed for legal assessment. As the more recently reported campaigns use vishing, help-desk impersonation, MFA and passkey-reset lures, spoofed support sites, and AI-enabled voice mimicry, those legal workflows should specify who is responsible for assessing regulatory notification obligations, contractual notices, law-enforcement engagement, litigation holds, board or committee updates, and potential enforcement or private-litigation exposure. Legal teams should also coordinate with outside counsel at the outset of any incident to preserve privilege over legal advice and incident-response workstreams, including forensic and other vendor engagements where appropriate.

4. *Assess Vendor, Contract, Insurance, and Regulatory-Tracking Readiness*: Evaluate whether key vendor agreements, data processing agreements, managed-service arrangements, and cloud or identity-provider contracts adequately address the threat scenarios reflected in recent cyberattacks. Reviews should consider cybersecurity reps and warranties, audit and cooperation rights, incident escalation procedures, breach-notice timing and content, regulator-facing support, evidence preservation, limitations of liability and indemnity coverage, and subcontractor obligations. Legal teams should confirm that cyber insurance notice, consent, panel-vendor, and privilege-related requirements are understood *before* an incident, so that claims processes do not conflict with legal strategy or regulatory-response obligations. Finally, relevant regulatory guidance, supervisory expectations, and enforcement trends affecting financial institutions, including developments tied to AI-enabled social engineering, account takeover, ransomware, and sector-specific threat-intelligence sharing, should be monitored on an ongoing basis.

5. *Conduct a Tabletop Exercise*: Conduct a tabletop exercise using realistic scenarios drawn directly from the current threat landscape. Tabletop exercises should involve cross-functional participation from legal, compliance, information security, business leadership, communications, and human resources, and should test not only technical response capabilities but also legal and regulatory notification obligations, insurance notice requirements, and stakeholder communications.

If you have any questions regarding this client alert, please contact the following attorneys or the Willkie attorney with whom you regularly work.

Daniel K. Alvarez	**Laura E. Jehl**	**Briony Pollard**	**Alexandra Barczak**
202 303 1125	202 303 1056	+44 20 3580 4716	202 303 1076
dalvarez@willkie.com	ljehl@willkie.com	bpollard@willkie.com	abarczak@willkie.com

WILLKIE

BRUSSELS CHICAGO DALLAS FRANKFURT HAMBURG HOUSTON LONDON LOS ANGELES
MILAN MUNICH NEW YORK PALO ALTO PARIS ROME SAN FRANCISCO WASHINGTON