Suggested Routing: *Anti-Money Laundering, Compliance, Cyber, Financial Crimes, Fraud, Information Technology, Operations, Risk, Senior Management and Supervision.*

Think Before You Sign: How Threat Actors Are Targeting Remote Document Signature Platforms

June 25, 2026

Email phishing schemes have challenged the financial industry for decades, resulting in billions of dollars in losses. FINRA has recently observed an increase in a specific type of email phishing scheme—one in which threat actors use remote document signature platforms (RDSPs), such as DocuSign, Dropbox Sign or ReadySign, to gather sensitive data and facilitate fraudulent payment requests.[1] Successful RDSP phishing schemes can result in significant financial and data losses for member firms and their customers. Notably, member firms that do not offer RDSP services remain vulnerable; threat actors impersonate these platforms to target their customers, exposing firms to substantial reputational harm when fraud occurs under their name. Threat actors sent an estimated 3.5 million RDSP-related malicious emails in 2024.

This Threat Intelligence Product (TIP) provides an overview of tactics threat actors are using in their RDSP phishing schemes and offers mitigation strategies for member firms, employees and customers.

Threat Overview

In an RDSP phishing scheme, threat actors send emails containing fraudulent documents and attachments from authentic RDSP accounts and mimic legitimate signature requests. These schemes have two primary goals: (1) gaining unauthorized access to recipients' devices to gather sensitive personal or financial data; and (2) facilitating fraudulent payment requests.

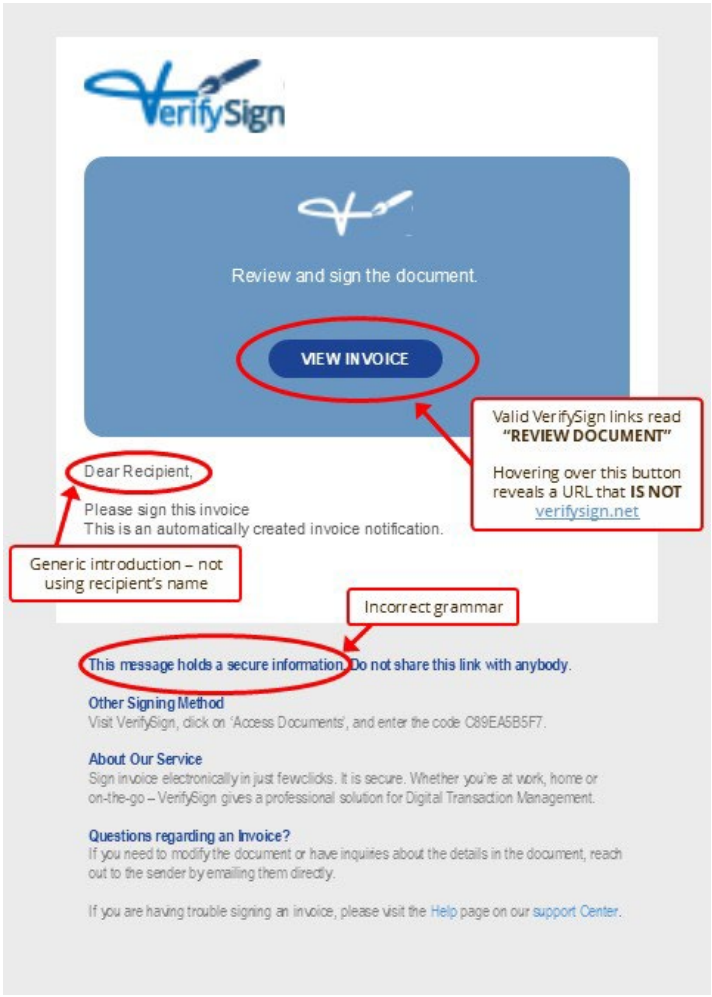
Threat actor tactics range from simple deception to advanced techniques, including artificial intelligence (AI)-powered attacks that incorporate deepfakes and personalized phishing.[2] These scams closely resemble authentic RDSP communications and use branding and formatting that can bypass conventional spam filters and potentially deceive even cautious recipients.

Listed below are several messaging or request examples a potential victim might receive as part of an RDSP phishing scheme:

- **Cryptocurrency and digital asset investments,** in which victims are encouraged to open digital wallets on fraudulent trading platforms, only for the threat actor to steal their funds and personal credentials.
- **Legal documents** (*e.g.*, letters of authorization, account applications, contracts) that require a signature and are often portrayed as time-sensitive to prevent financial penalties.

- **Marketing offers** featuring unrealistic or misleading giveaway prizes, rewards or payouts—requiring a signature to receive them—sometimes using the branding of legitimate companies.
- **Debt relief or lending offers**, such as loan modifications, debt forgiveness, or financial assistance programs.
- **Technical support services**, such as anti-malware software or computer repair services.
- **Subscription renewals** requiring payment.
- **Economic relief programs**, such as government benefits, stimulus programs, or financial hardship assistance.
- **Employment opportunities**, such as work-from-home postings or requests for personal information.[3]

As AI tools become increasingly accessible, threat actors leverage this technology to analyze publicly available information—such as social media profiles, professional networks and public records—to craft highly personalized phishing messages tailored to individual victims. **Below is an example of an RDSP phishing email sent by threat actors, with suspicious elements circled and annotated:**



Strategies to Mitigate the Threat

Member firms may consider the following practices to mitigate RDSP phishing risks:

Technical Security Controls

- Strengthen email security controls by configuring systems to include:
  - flagging emails from domains that mimic RDSP platforms;
  - scanning for malicious links, attachments and suspicious sender patterns; and
  - utilizing Domain Name System (DNS) filtering to block known malicious domains that impersonate RDSPs.[4]
- Maintain current security infrastructure by ensuring timely updates to endpoint detection systems and comprehensive incident response plans that include:[5]
  - defining clear escalation procedures, including time-sensitive response requirements;
  - creating an incident reporting documentation log; and
  - conducting post-incident analysis to identify potential threats.

Operational Procedures

- Employ identity verification protocols to confirm that customer signatures match existing information on file, such as name, address, email address and existing signature associated with the customer.
- Develop a threat monitoring system for RDSP-related cybersecurity risks that may incorporate elements such as:
  - conducting ongoing analysis of RDSP-related threats;
  - tracking emerging techniques used by threat actors; and
  - updating security protocols based on new intelligence.
- Establish clear reporting channels for suspected RDSP phishing attempts, including:
  - notifying the targeted RDSP platform for all incidents;
  - alerting internal cybersecurity teams when employees are affected;
  - informing customer email service providers when clients are targeted; and
  - maintaining a centralized incident tracking and response log.

Education and Training

- Educate customers about legitimate member firm communications by providing clear expectations of email content and timing, including explicitly stating what information the member firm will never request from a customer via email.
- Recommend customers access documents securely by navigating directly to the RDSP's official website, using unique security codes provided by the platform, rather than using QR codes or email links. Similar guidance for firm employees can be included in the firm’s RDSP request protocols.
- Encourage customers to review all message components (*e.g.*, sender information, subject line and body) for red flags, including grammatical or typographical errors, signs of bulk distribution,

generic greetings, urgent or pressuring language and unsolicited attachments. Similar guidance should be included in training provided to firm employees.

- Train firm employees on identifying potential RDSP phishing attempts and the associated risks.

Reporting Phishing Attempts and Other Cybersecurity Events

FINRA encourages member firms to report cybersecurity events, including phishing attempts, to:

- the FBI using its Internet Crime Complaint Center or by calling 1-800-CALLFBI (1-800-225-5324);
- the Federal Trade Commission through its website for reporting fraud, scams and bad business practices, ReportFraud.ftc.gov;
- FINRA using the Regulatory Tip Form; and
- the SEC using the Tips, Complaints, and Referrals form or by calling (202) 551-4790.

FINRA's Financial Intelligence Unit (FIU) supports the protection of investors and markets by identifying and assessing threats and trends impacting the financial and securities industry and disseminating actionable intelligence.

This TIP was prepared by FINRA's FIU. It is based on internal data and open-source information. Questions may be directed to FIU@finra.org.

This TIP does not create new legal or regulatory requirements or new interpretations of existing requirements, nor does it relieve firms of any existing obligations under federal securities laws, regulations and FINRA rules. Member firms may consider the information in this TIP in developing new, or modifying existing, policies and procedures that are reasonably designed to achieve compliance with relevant regulatory obligations based on the member firm's size and business model. Moreover, some information may not be relevant due to certain firms' models, sizes, or practices.

---

[1] FINRA is not endorsing any commercial product or service. Any reference to specific commercial products, processes, or services does not constitute or imply their endorsement, recommendation or favoring by FINRA.
[2] Other examples include social engineering, malicious generative pre-trained transformers (known as GPTs—large language models pre-trained on a vast amount of text data to generate human-like text across a variety of tasks (*e.g.*, translating languages, answering questions, generating content)), ransomware, and other adversarial uses of AI and machine learning.
[3] Work-from-home schemes use fake job opportunities to extract upfront fees or personal information from victims.
[4] DNS filtering uses the Domain Name System to prevent employees from accessing malicious websites and harmful content.
[5] Incident Response Protocols are structured plans that outline how to respond to and manage cybersecurity threats. These plans generally involve six phases: Preparation, Identification, Containment, Eradication, Recovery and Lessons Learned.