

SECURITY NOTICE

The Office of the Commissioner of Insurance of Puerto Rico (OCIPR) alerts all regulated entities about an active phishing campaign involving fraudulent emails, identified by the National Insurance Producer Registry (NIPR), targeting insurance producers. These emails reference **alleged overdue invoices** and may appear to originate from legitimate or trusted domains, including entities such as the National Association of Insurance Commissioners (NAIC) or the Stripe payment platform.

These messages are **fraudulent** and **have not been sent from official NIPR accounts**. Any unexpected or unsolicited invoice should be considered suspicious. For more information, please refer to NIPR's official notice: <https://nipr.com/nipr-phishing-awareness>

How to identify a fraudulent email?

- Verify the sender's address (look for subtle variations in domains)
- Be cautious of generic greetings such as "Dear Customer"
- Review the tone: grammatical errors or excessive urgency
- Avoid clicking on suspicious links (verify their destination)
- Confirm directly with the entity before taking any action

Recommended security measures for regulated entities

- Do not respond to or take action on unsolicited invoices
- Do not open suspicious links or attachments
- Do not issue payments without prior validation
- Carefully verify the authenticity of the sender
- Implement internal controls for payment validation
- Train staff on phishing risks
- If in doubt, contact NIPR directly: niprbillingdept@nipr.com

References and best practices

Adoption of guidance from the following entities is recommended:

- Cybersecurity and Infrastructure Security Agency (CISA)
- Federal Trade Commission (FTC)
- National Institute of Standards and Technology (NIST)

The OCIPR appreciates your immediate attention and urges all regulated entities to remain vigilant in protecting the insurance sector against fraud and cyber threats.