CALIFORNIA
BANKERS
ASSOCIATION

SOCIAL MEDIA TOOKIT

2026 INTERNATIONAL FRAUD AWARENESS WEEK

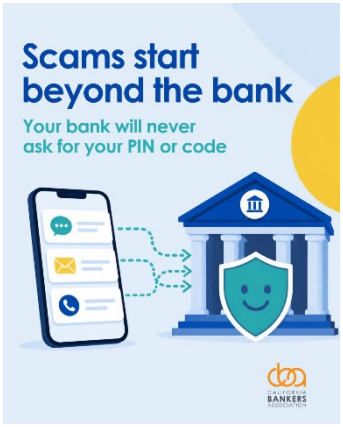
November 15-21

Introduction

International Fraud Awareness Week runs November 15–21, and this toolkit gives you five ready-to-post messages for the week. Each post pairs a practical consumer tip with a clear message about what banks are doing to stop fraud, and why stopping it takes partners across many industries. Post as written or personalize adding your own approved resources and logo. Questions? Contact Samantha DeMelo, CBA Communications Manager, at sdemelo@calbankers.com.

POST 1: SCAMS START BEYOND THE BANK

IMAGE



Download Image

- Facebook/IG
- X

SOCIAL COPY

Facebook

Most scams don't start at the bank. They start with a phone call, a text, an email or a message on social media.

That's why banks are working to stop fraud at every step, and why stronger partnerships with other industries matter.

You can help, too. If someone contacts you asking for your password, PIN or a one-time code, stop. [BANK NAME] will never ask for these. Hang up and call us at the number on the back of your card.

#FraudWeek #FraudAwarenessWeek #ScamPrevention

Instagram

That urgent call from "your bank"? It may not be your bank.

Most scams start far from the bank: a phone call, a text, an email or a social media message. Banks are working every day to stop fraud, and stronger partnerships across industries help stop it sooner.

Here's your part: [BANK NAME] will never ask for your password, PIN or one-time code. If anyone does, pause. Hang up. Call the number on the back of your card.

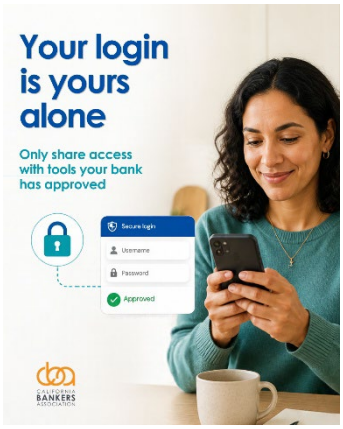
#FraudWeek #FraudAwarenessWeek #ScamPrevention

X

Most scams start on a phone, text or social feed before they ever reach a bank. Stopping them takes stronger partnerships. Tip: Your bank will never ask for your password, PIN or one-time code. Pause and verify. #FraudWeek #FraudAwarenessWeek

POST 2: PROTECTING ACCOUNTS FROM UNAUTHORIZED AI AGENTS

IMAGE



Download Image

- Facebook/IG
- X

SOCIAL COPY

Facebook

AI tools are everywhere, and some promise to manage your money for you. An "AI agent" is a program that can take actions on its own, like logging in or moving money.

When an AI agent your bank hasn't approved gets your login, it can open the door to mistakes or fraud. That's why banks are restricting unauthorized third-party AI agents from accessing customer accounts. It's one more way banks are acting now to prevent unauthorized transactions.

Keep your login to yourself. Only use tools and services your bank has approved. Not sure? Ask us!

#FraudWeek #FraudAwarenessWeek #AIFraud

Instagram

Your banking login is yours alone. Keep it that way.

Some apps and AI tools ask for your bank username and password so they can act on your behalf. If your bank hasn't approved them, that's a risk.

Banks are restricting unauthorized third-party AI agents from accessing customer accounts. It's part of how we are acting now to keep your money safe and prevent unauthorized transactions.

Before you connect any tool to your account, check with us.

#FraudWeek #FraudAwarenessWeek #AIFraud

X

Banks are restricting unauthorized AI agents from accessing customer accounts to help stop unauthorized transactions. Tip: Don't give your banking login to any app or AI tool your bank hasn't approved. #FraudWeek #FraudAwarenessWeek

POST 3: GETTING AHEAD OF AI-POWERED SCAMS

IMAGE



Download Image

- Facebook/IG
- X

SOCIAL COPY

Facebook

Scammers are using AI to copy voices and create fake videos that look and sound like someone you love. A call from a "grandchild" in trouble or a "boss" who needs money fast may not be real.

Banks are getting ahead of these threats. They are working with other industries, critical infrastructure providers and regulators to find AI risks early and reduce them.

You can protect your family today: pick a safe word only you know. If a call feels urgent or strange, hang up and call back on a number you already have.

#FraudWeek #FraudAwarenessWeek #AIFraud

Instagram

It sounds like your grandson. It might not be him.

AI can now copy a voice or face in minutes. Banks are working with other industries, critical infrastructure providers and regulators to spot these risks early and reduce them.

Three steps for your family:

1. Pick a safe word only you know.

2. Ask for it on any urgent call.

3. Hang up and call back on a number you trust.

Talk about it at your next family dinner.

#FraudWeek #FraudAwarenessWeek #AIFraud

X

Banks are working with other industries, critical infrastructure providers and regulators to get ahead of AI risks. Tip: A voice can be faked. Use a family safe word, and hang up and call back on a number you know. #FraudWeek #FraudAwarenessWeek

POST 4: FRAUD PREVENTION IS A TEAM EFFORT

IMAGE



Download Image

- Facebook/IG
- X

SOCIAL COPY

Facebook

No single company can stop fraud alone. Scams move across phone networks, apps, social media, online marketplaces and stores before they reach a bank.

That's why fraud prevention takes a team: phone carriers, tech and social media platforms, retailers, government and banks all working together. When every partner does its part, scams get stopped sooner.

You're part of the team, too. When you see a scam text, fake ad or phony profile, report it on the platform where you found it. Every report helps protect someone else.

#FraudWeek #FraudAwarenessWeek #ScamPrevention

Instagram

Stopping scams is a team sport.

Scams travel through phones, apps, social feeds and online stores before they ever reach a bank. Stopping them takes every industry working together: carriers, tech platforms, retailers, government and banks.

You have a spot on the team. See a scam text, a fake ad or a phony profile? Report it on the app or site where you saw it. It only takes a few taps, and it can protect your friends and neighbors.

#FraudWeek #FraudAwarenessWeek #ScamPrevention

X

Fraud prevention takes a team: phone carriers, tech and social media platforms, retailers, government and banks. Tip: Report scam texts, ads and fake profiles right where you see them. #FraudWeek #FraudAwarenessWeek #ScamPrevention

POST 5: YOUR BANK IS YOUR PARTNER

IMAGE



Download Image

- Facebook/IG
- X

SOCIAL COPY

Facebook

Remember this: you don't have to face scams alone.

Banks are working every day to protect customers, from limiting unauthorized AI agents to partnering with other industries, critical infrastructure providers and regulators to stop scams sooner.

If something doesn't feel right, act fast. Contact us using the number on the back of your card or on our official website. Then report the scam at ReportFraud.ftc.gov. The sooner you reach out, the sooner we can help.

#FraudWeek #FraudAwarenessWeek #ScamPrevention

Instagram

Something feel off? Call us first.

Banks are working every day to protect you, and we're partnering with other industries and regulators to stop scams before they start.

If you think you've been targeted:

1. Contact us using the number on your card or our official website.

2. Report it at ReportFraud.ftc.gov.

3. Tell a friend or family member so they can watch for the same scam.

The sooner you reach out, the sooner we can help.

#FraudWeek #FraudAwarenessWeek #ScamPrevention

X

Banks are working every day, with partners across industries, to stop fraud. Think you've been targeted? Call your bank right away using the number on your card, then report it at ReportFraud.ftc.gov. #FraudWeek #FraudAwarenessWeek