



STOP. VERIFY. REPORT.

Protect Yourself Against Fraud and Scam Attempts

Fraudsters are becoming increasingly sophisticated, using phone calls, text messages, emails, and fraudulent websites to impersonate banks, government agencies, and other trusted organizations.

The FBI has warned that criminals frequently use caller ID spoofing, social engineering, and fake websites to gain access to accounts and steal funds.



STOP.

Pause and be cautious
with unexpected
communications.



VERIFY.

Confirm the request
using trusted channels
before taking any action.



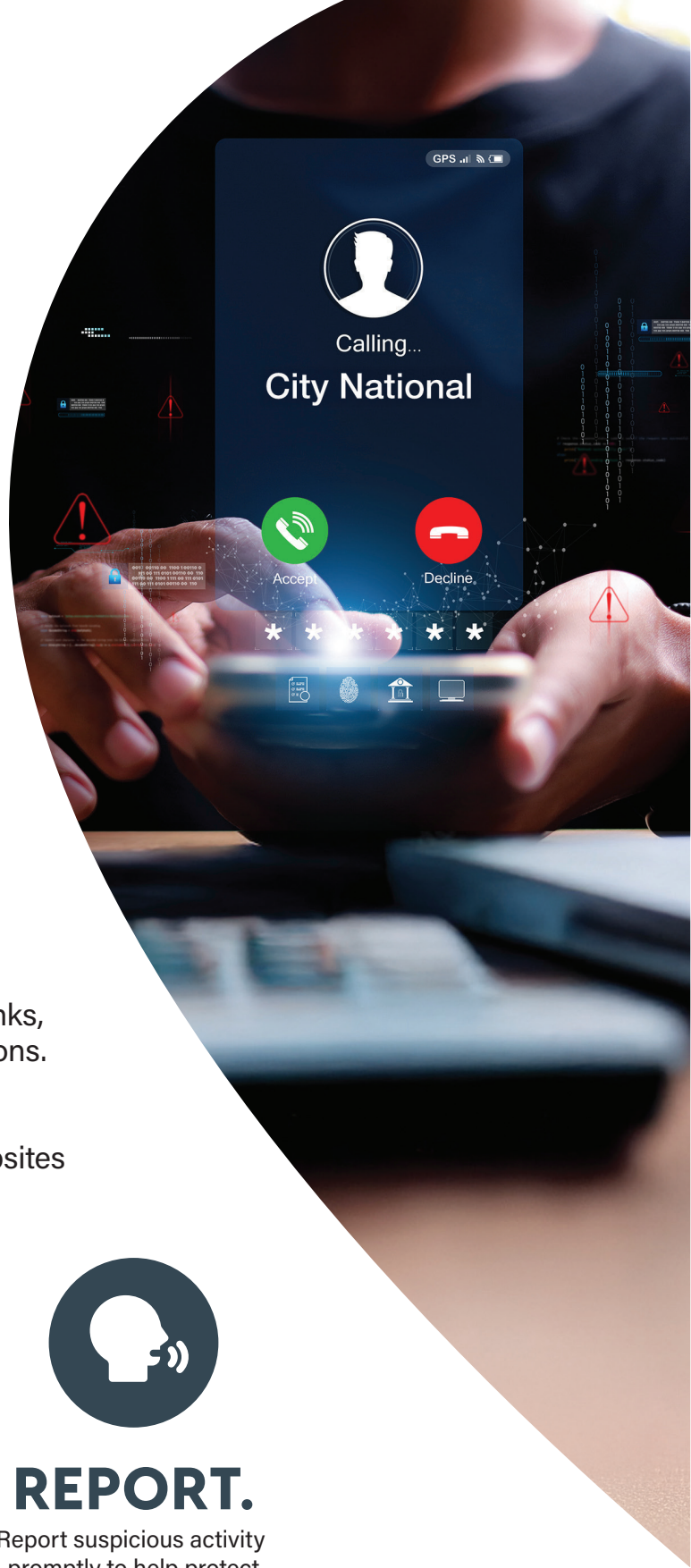
REPORT.

Report suspicious activity
promptly to help protect
your accounts.

Your Best Defense Is Awareness

Technology plays an important role in detecting suspicious activity, but many scams rely on manipulating trust and creating urgency.

Taking a few moments to verify a request before responding can help prevent financial loss and protect your personal and financial information.





STOP.

If you receive an unexpected communication regarding your account, a payment, suspicious activity, or a request for information, take a moment to pause before taking any action.

Fraudsters often create a false sense of urgency, hoping you will act before verifying the request.



VERIFY.

Before responding, ask yourself:

- Was I expecting this communication?
- Am I being asked to provide sensitive information or approve a transaction?
- Is the sender pressuring me to act immediately?
- Does something about this request seem unusual?

To protect yourself:

- ✓ Contact the Bank using a trusted phone number that you obtain independently.
- ✓ Confirm requests directly with your Relationship Manager, Client Service Associate, or the Client Concierge Center.
- ✗ Do **not** click links in unsolicited emails or text messages.
- ✗ Do **not** open unexpected attachments.
- ✗ Do **not** call the phone number provided in the email, text message, or request.
- ✗ Do **not** share passwords, PINs, one-time passcodes, security tokens, or multifactor authentication (MFA) codes.



City National Bank of Florida will **NEVER** ask you to provide your password, MFA code, security token, or online banking credentials.



REPORT.

If you receive a suspicious email, text message, or phone call:

- Stop the interaction immediately.
- Do not provide any information.
- Do not click any links or attachments.
- Contact the Bank through a trusted channel.
- Report the incident promptly so we can help protect your accounts and investigate potential fraud.

Before you respond to any unexpected request involving your money or personal information, remember three simple steps:

STOP. VERIFY. REPORT.

When in doubt, contact your Relationship Manager, Client Service Associate, or the Client Concierge Center directly using a trusted phone number. A brief verification today could prevent a significant loss tomorrow.



NMLS #412469
Member FDIC



citynational.com