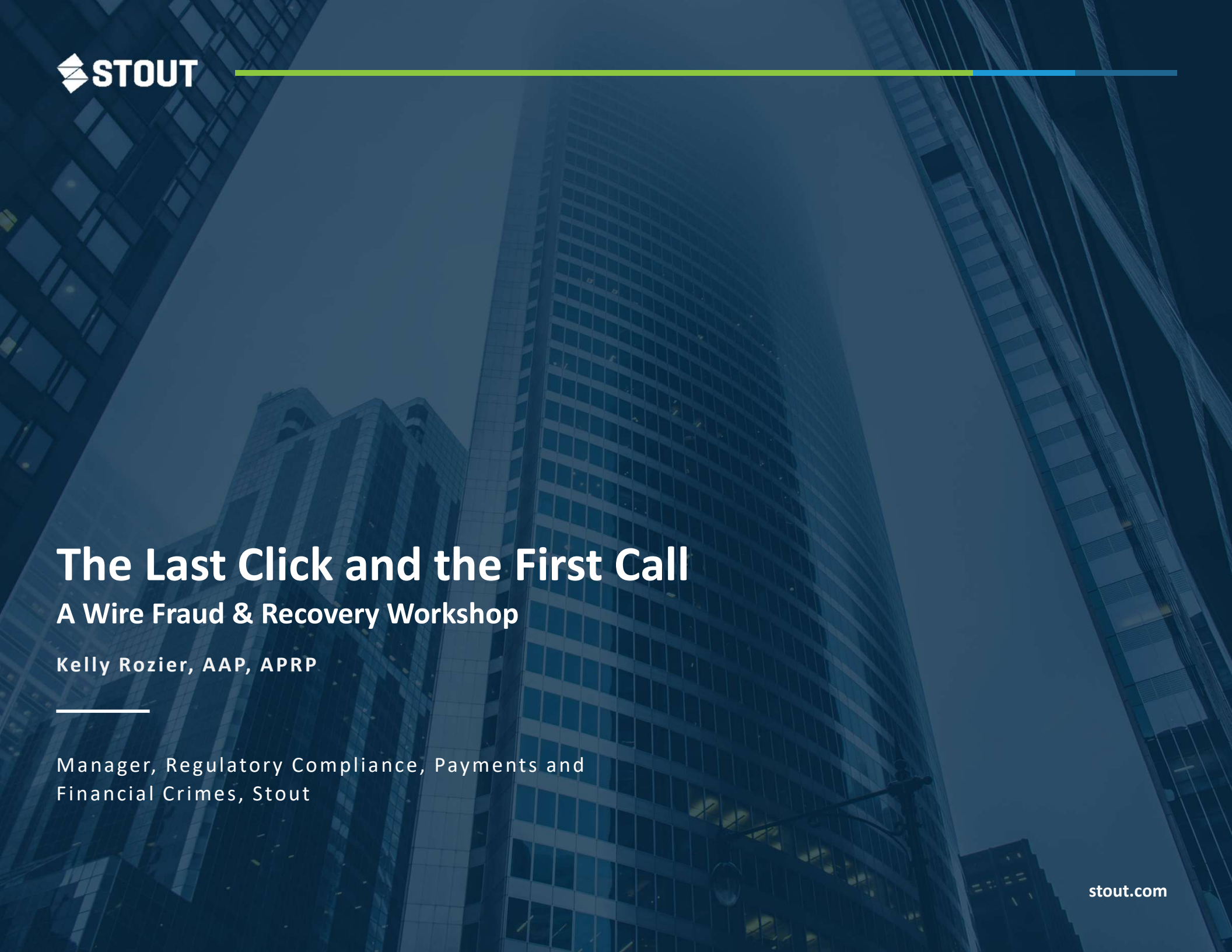


# The Last Click and the First Call

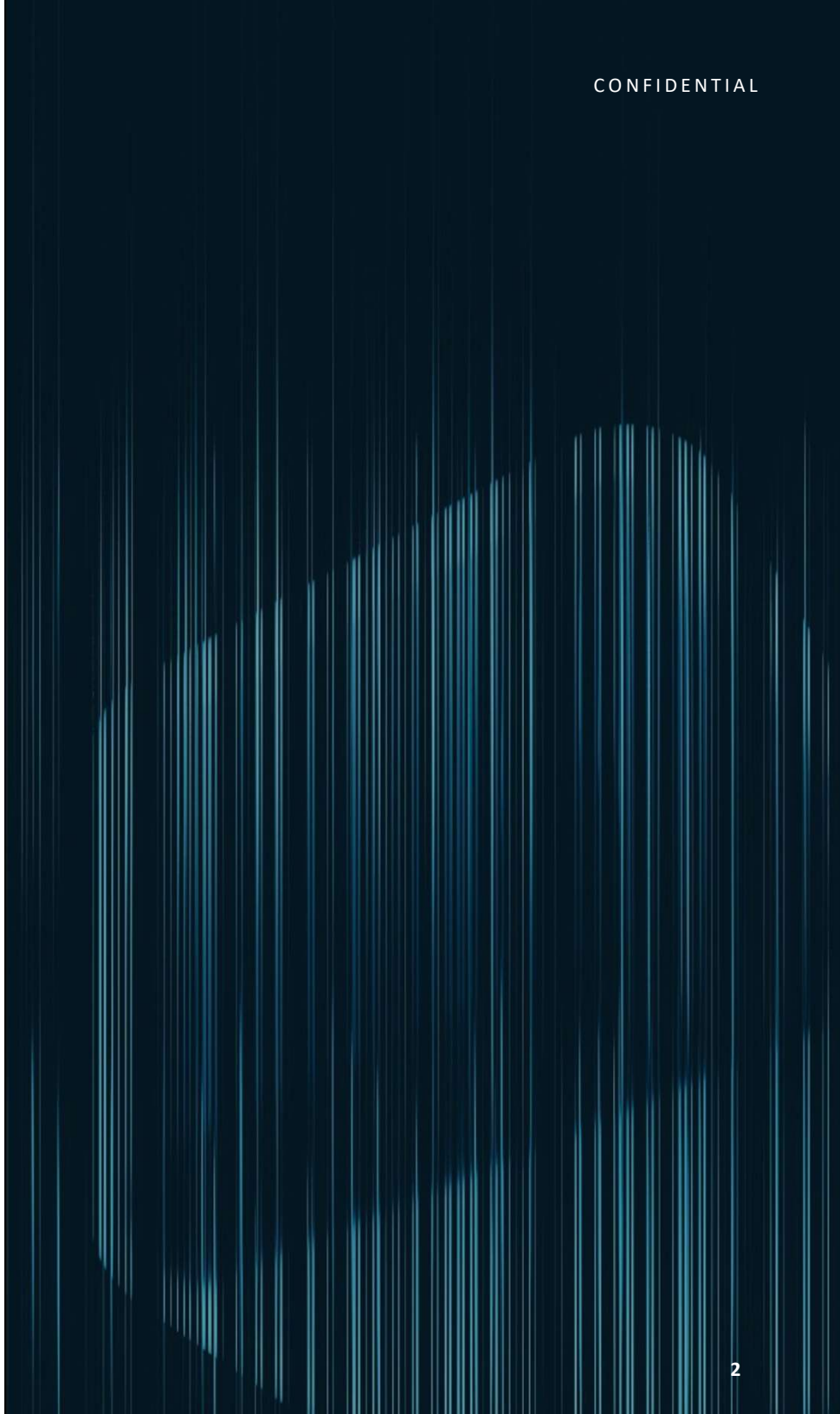
## A Wire Fraud & Recovery Workshop

**Kelly Rozier, AAP, APRP**

Manager, Regulatory Compliance, Payments and Financial Crimes, Stout

# Agenda

1. Introduction
2. Anatomy of a Wire Fraud Loss
3. Part 1: The Last Click — Pre-Release Controls
4. Part 2: The First Call — Recovery & Response
5. Key Takeaways & Discussion



SECTION 1

# Why This Matters

**$3.05B**

BEC losses reported to the FBI IC3 in 2025, up from $2.77B in 2024

**86%**

of BEC losses move through wire or ACH transfers

**24–72 hrs**

the realistic window for wire recovery once funds move

**58%**

success rate of the FBI Recovery Asset Team when funds are frozen quickly

*Every gap in a pre-release control, and every minute lost after discovery, shows up in these numbers.*

*Source: FBI Internet Crime Complaint Center (IC3), 2025 Internet Crime Report*

SECTION 1

# Anatomy of a Wire Fraud Loss


**Initiation**
Fraudulent instructions arrive by email, call, or portal

**Approval**
The last click before release — the final control point

**Release**
Wire sent via Fedwire or SWIFT

**Discovery**
Fraud identified — the first call starts the clock

**Window Closes**
Funds layered and dispersed across accounts

**Today's focus: Part 1 examines stage 2 (the last click before release). Part 2 examines stage 4 (the first call after discovery).**

PART I

# The Last Click

## Pre-Release Controls & Escalation

CASE STUDY 1

# Setting the Scene

ABC Manufacturing's controller receives an email from the company's longtime steel supplier: remittance details have changed ahead of a $340,000 invoice payment.

The email matches prior threads, uses the supplier's usual tone, and cites a real outstanding invoice number. The sending domain is one character off from the supplier's actual domain.

**The controller forwards the new instructions for approval.**

## CASE FILE

**Company:** Mid-size manufacturer, ~$60M revenue

**Fraud Type:** Vendor email compromise (VEC)

**Amount:** $340,000

**Channel:** Outbound wire, same-day release

**Trigger:** “Updated remittance instructions” email

CASE STUDY 1

# The Approval Moment

## What the Approver Saw

- Email thread matched the ongoing vendor conversation
- Invoice number referenced was legitimate and outstanding
- Message used the vendor's normal tone and signature block
- Request was framed as routine, time-sensitive account maintenance

## What Was Missing

- Sending domain was one character off from the vendor's real domain — never checked
- No callback made to a verified phone number on file
- Dual approval was waived because the vendor was “trusted”
- Sanctions/OFAC screening skipped under time pressure

*Discussion: which of these gaps exists in your current wire approval workflow?*

# Exercise: Spot the Gap — as a group, identify three controls that would have stopped this wire before release.

> Think through the gaps on your own, then we'll open the floor — name the specific control, who owns it, and where it sits in the approval workflow.

CASE STUDY 1

# Effective Pre-Release Controls

## Dual Control & Segregation of Duties

No single person can both initiate and release a wire, regardless of vendor tenure or trust.

## Verified Callback

Any change to payment instructions triggers a call to a number on file — never a number in the request.

## Sanctions & OFAC Screening

Every outbound wire is screened before release, with no exceptions for time pressure.

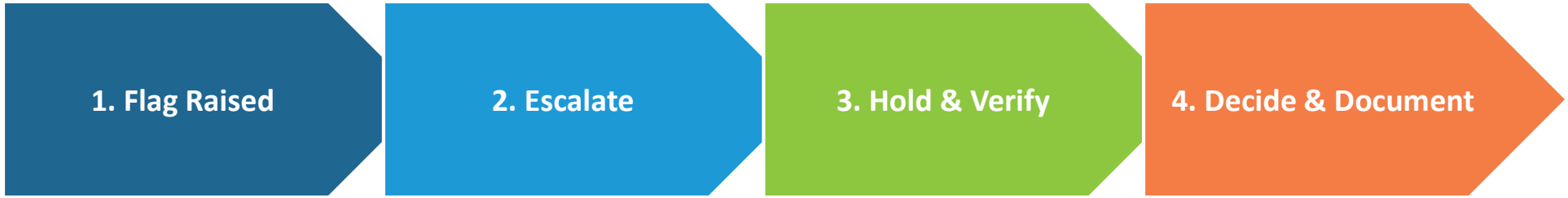
## Wire Limits

Dollar thresholds trigger additional review; unusual destinations flag for manual hold.

*Each control closes one of the gaps from the case file.*

CASE STUDY 1

# Escalation Protocols Before Release




| | | | |
|---|---|---|---|
| Approver notices a red flag or has any doubt about the request | Route immediately to a second approver or the fraud/AML team | Release is paused pending out-of-band verification | Release or reject, and log the rationale in the file |

**The rule: no one is penalized for escalating a false alarm. Everyone is accountable for skipping this step.**

PART II

# The First Call

## Recovery & Response

CASE STUDY 2

# Discovery

Three business days later, the real steel supplier calls: their invoice is still unpaid. ABC's treasury team pulls the wire confirmation and realizes the $340,000 went to an account the supplier has never used.

By the time anyone picks up the phone, the funds have already sat at the receiving bank for three days, well past the window when a same-day recall request is most effective.

**The first call starts the clock — and it should have started three days earlier.**

## DISCOVERY TIMELINE

**Day 0:** Wire released, $340,000 to fraudulent account

**Day 3:** Legitimate supplier calls about unpaid invoice

**Day 3, +2 hrs:** Fraud confirmed internally, first call not yet made

**Day 3, +2.5 hrs:** Bank notified — recall request filed

CASE STUDY 2

# The Golden Hour: First Actions

## First 30 Minutes

- Escalate immediately to your institution's fraud or wire department — do not email
- Request an immediate wire recall from the receiving bank
- Notify internal fraud, compliance, and legal teams
- Preserve the original email, headers, and any call recordings

## Within 24 Hours

- File a complaint at ic3.gov for FBI Recovery Asset Team review
- Notify your cyber insurance carrier of a potential claim
- Contact the receiving bank's fraud department, not just your own
- Do not tip off the suspected fraudster by replying to their email

*Every one of these steps should already have an owner and a phone number before fraud happens.*

CASE STUDY 2

# Recovery Mechanics

## The Recall Request

- Sent to the receiving bank via Fedwire or SWIFT (MT192 / camt.056)
- Success depends entirely on whether the funds are still on deposit

## The Closing Window

- Recovery odds drop sharply after 24 hours as funds are split or converted
- The FBI Recovery Asset Team can request a hold if notified fast enough

## UCC Article 4A

- Governs U.S. commercial wire transfer liability
- A properly authorized wire generally isn't the bank's liability, even if fraud-induced
- Liability can shift if the bank skipped its own agreed security procedures

CASE STUDY 2

# Coordination Map

# Exercise: Build the Recovery Timeline — sequence the first 24 hours from the moment fraud is confirmed.

10 minutes. As a room, call out who you'd contact first, second, and third and name the one piece of information each call needs to be effective.

RECAP

# Key Takeaways Checklist

## Before You Approve

- ✓ Dual control on every wire, with no exceptions for trusted vendors
- ✓ A verified callback to a number on file before any instruction change
- ✓ Sanctions screening on every outbound wire, regardless of time pressure
- ✓ A clear escalation path where flagging a false alarm carries no penalty

## After You Discover

- ✓ A named first call, with a phone number, before fraud ever happens
- ✓ A recall request filed with the receiving bank within the golden hour
- ✓ An ic3.gov complaint and insurance notice within 24 hours
- ✓ A coordination plan across internal teams, banks, and law enforcement

*If any box is unchecked, that's this quarter's action item.*

WRAP-UP

# Discussion & Q&A

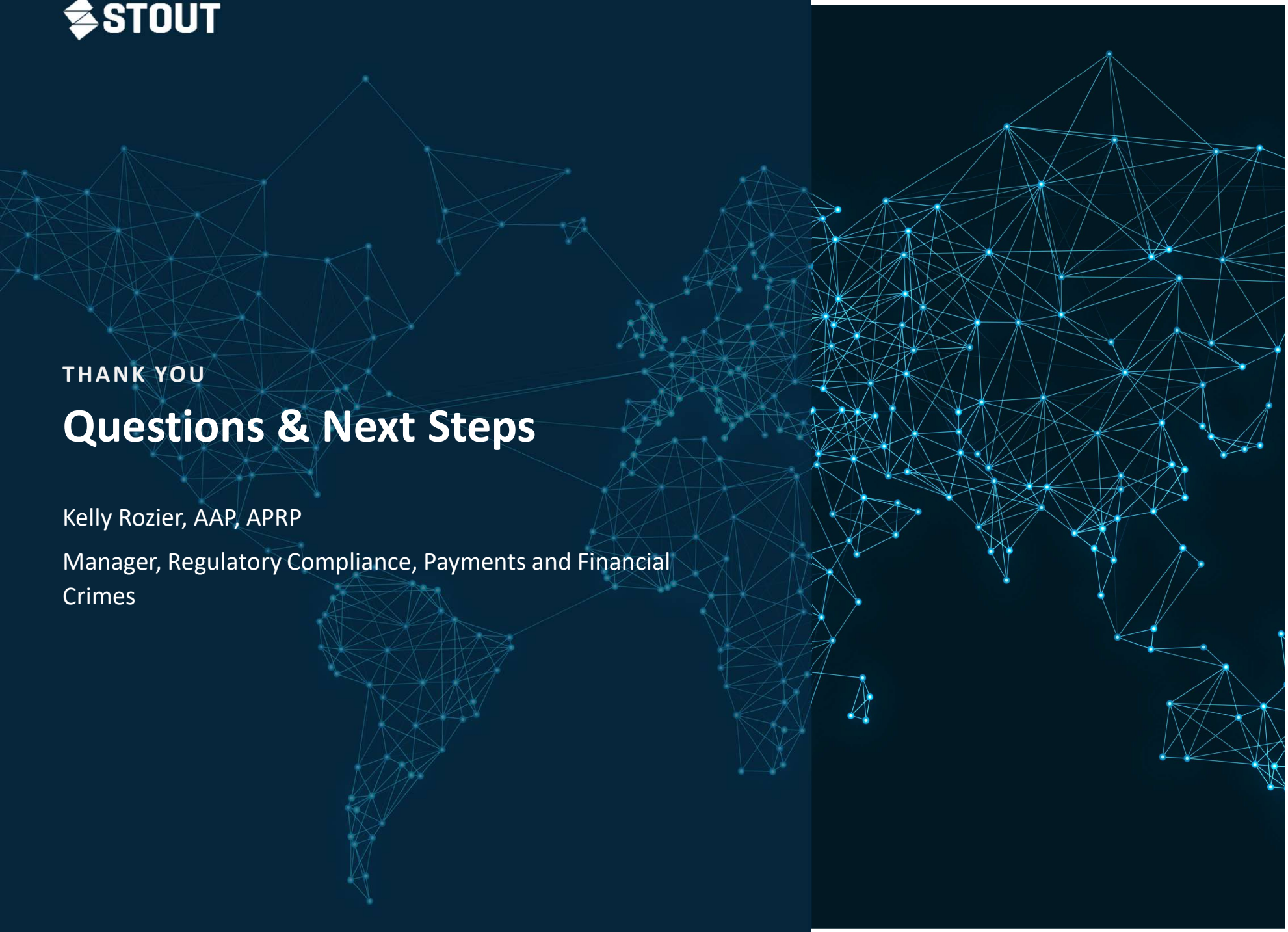
1. Where in your wire approval workflow could a “trusted vendor” exception bypass a control?

2. Who is your organization's designated first call, and do frontline staff know that number today?

3. How would your team notify the receiving bank and file an IC3 complaint within the golden hour?

4. What would it take to get callback verification and sanctions screening to zero exceptions?

STOUT



RELENTLESS EXCELLENCE®

THANK YOU

# Questions & Next Steps

Kelly Rozier, AAP, APRP

Manager, Regulatory Compliance, Payments and Financial Crimes