Urgency, Deception, and Big Losses:
How Criminals Trick Businesses Every Day

RENASANT | SMITH+HOWARD Advisory LLC

Oliver Villacorta

Senior Manager, Cyber Risk Management + Compliance | Smith + Howard

Oliver is a cybersecurity and compliance leader advising organizations nationwide on how to assess, manage, and mitigate cyber risk. As a Senior Manager in Smith + Howard's Cyber Risk Management + Compliance practice, he specializes in helping middle-market and PE-backed companies build resilience, align to industry frameworks, and prepare for evolving threats.

He has presented cybersecurity risk to leaders at major financial institutions including Cadence Bank, JPMorgan Chase, and Bank of America, as well as to executives in the manufacturing sector. Oliver's expertise includes NIST CSF, ISO 27001, HITRUST, cyber risk assessments, and healthcare privacy and security.

He holds multiple advanced certifications including CISSP, CCSP, SSCP, HCISPP, and ISO 27001 Lead Auditor, and has degrees from the University of North Georgia, Kennesaw State University, and Georgia State University.

SMITH+HOWARD
Advisory LLC

Why This Matters

Fraud isn’t seasonal anymore. It’s daily. It’s constant. And it’s hitting businesses that thought “it would never happen to us.”

Key facts:

- 79% of organizations experienced payments fraud in 2024
- 63% experienced check fraud — still the #1 fraud type
- Wire transfers are now the #1 target for BEC attacks (63%)
- Only 22% of companies recover 75% or more of stolen funds

Renasant insight: The Treasury Solutions team now sees fraud attempts every single day — not just around the holidays.

Bottom line: Cyber + fraud = a financial risk, and human error is still the fastest path to loss.

RENASANT | SMITH+HOWARD Advisory LLC

The Two Most Common Attacks Hitting Businesses Right Now

1. Business Email Compromise (BEC)

- Slight domain misspelling (one letter transposed)
- Spoofed logos, signatures, and “urgent” invoice-change requests
- Requests to bypass normal controls (“Do this now — this is confidential”)
- Criminals often know birthdays, SSNs, or internal details from the dark web, making the call/email feel legitimate

2. “Vishing” — Phone-Based Fraud

Criminals now:

- Impersonate Renasant staff
- Use recorded **Renasant hold music**
- Use real employee names
- Use spoofed caller IDs
- Create urgency (“Someone is committing fraud on your account **right now**… I see them at the branch”)

If you get a toll-free call from Renasant?
Hang up immediately. Renasant does not call from 800 numbers.

RENASANT | SMITH+HOWARD Advisory LLC

What Must Happen for Fraudsters to Steal your $

1. Initial Contact

- Email or phone call appears legitimate (spoofed, urgent, familiar).
- Weak point: Lack of verification → recipient keeps engaging.

2. User Action

- Clicking a link, providing information, or changing payment instructions.
- Weak point: Not calling back on a verified number.

3. Payment Execution

- Money leaves the account before controls catch it.
- Weak point: No callback verification, no dual control, or “rubber-stamping” approvals.

Interrupt any one of these steps, and the fraud fails. (The “Fraud Kill Chain”)

RENASANT | SMITH+HOWARD Advisory LLC

Real Cases from Renasant Bank

RENASANT | SMITH+HOWARD Advisory LLC

RENASANT | SMITH+HOWARD Advisory LLC

Case 1

Invoice Change Scam Business Email Compromise (BEC)

- Email looked perfect: logo, signature, thread history.
- Single transposed letter in the email address.
- Client changed payment (routing) info without verifying.
- Loss: high, partial recovery.

Point: One missed detail = money gone.

RENASANT | SMITH+HOWARD Advisory LLC

Case 2

Fraudster Using Real Renasant Hold Music

- Criminal called pretending to be “Sarah from Treasury Support.”
- Put the client “on hold” and played recorded Renasant hold audio.
- Tried to move funds into a “safe account.”
- Client hesitated → hung up → called Renasant → scam stopped.

Point: Caller ID and hold music can be faked.

RENASANT | SMITH+HOWARD Advisory LLC

Case 2

Employee ACH Fraud

- Fired employee used valid credentials to send unauthorized ACH transactions.
- Police involved.
- 50% of funds recovered.

Point: Termination procedures must include immediate credential revocation.

What the Data Shows

Business Email Compromise (BEC) Dominates

- BEC accounts for 90%+ of all fraud incidents
- Invoice change fraud + urgent wire requests are the primary patterns

Wires Are Becoming High-Value Targets

- Several wire attempts exceed $90k–$250k
- Phone-based wire fraud (“vishing”) shows up multiple times in August–September

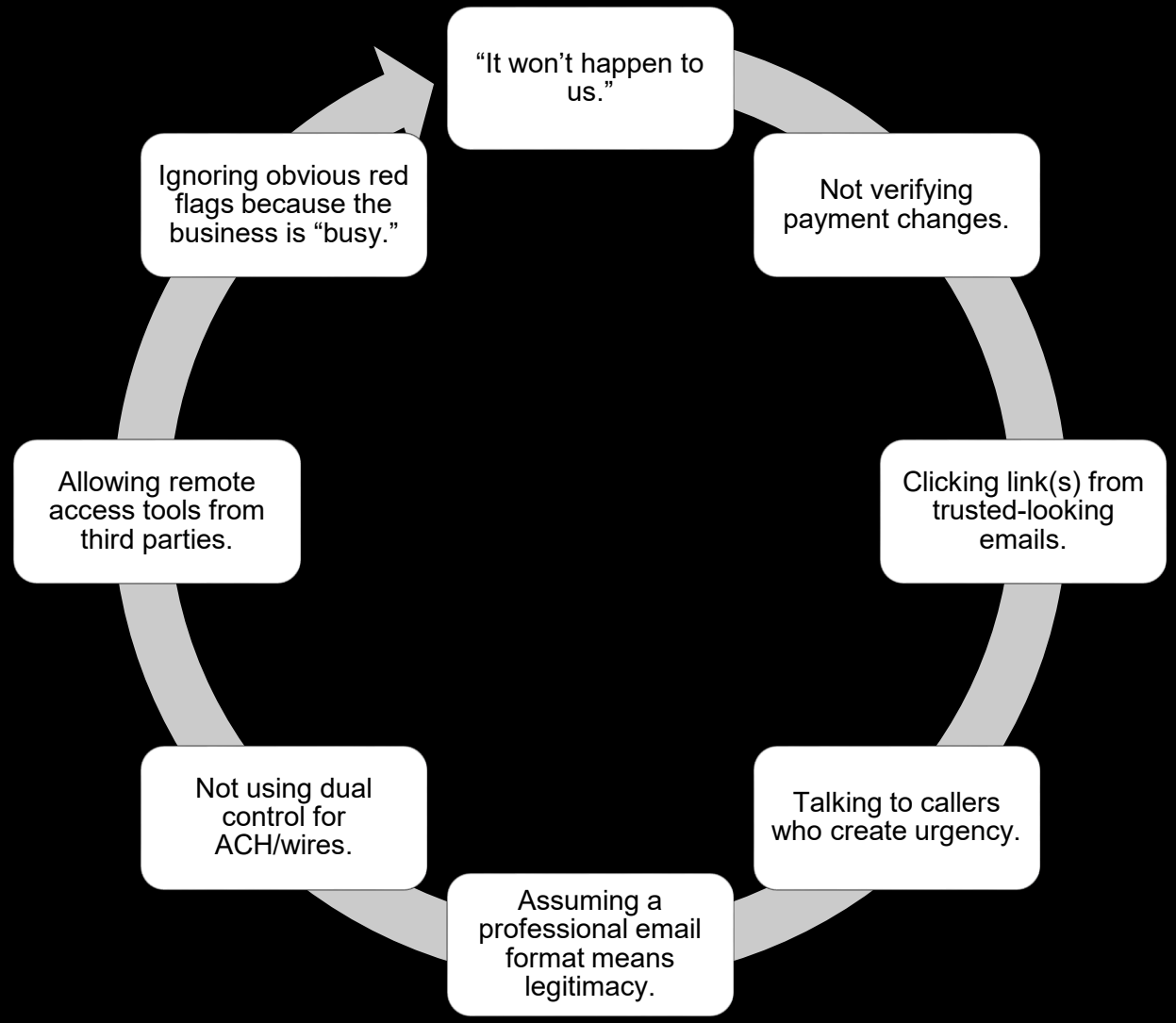
Recovery Rates Vary Widely

- Some cases recover 100%
- Many large ACH/BEC cases recover $0

What Businesses Get Wrong

“People aren’t losing money because technology failed.

They’re losing money because they didn’t stop to verify.”



Controls That Stop Fraud Cold

Dual Control ALWAYS

No wire/ACH should go out without a second approval.

Callback Verification

Using known numbers only

Never the number provided in the email

Strict Vendor Change Protocols

Every vendor change requires a callback to a known contact

No exceptions during "urgent" requests

Never Click Links in Unexpected Emails

"It's almost at the point we need to tell people: don't click anything."

No Toll-Free Call Acceptance

Hang up immediately.

No Remote Access: Ever!

Renasant will never request access to your machine

Use Bank Fraud-Mitigation Services

Check Positive Pay

ACH Positive Pay

Alerts

RENASANT | SMITH+HOWARD Advisory LLC

Holiday-Season Red Flags

Expect these tactics November–January:

- Urgent payment requests
- “I’ll lose my job if this isn’t paid today” language
- Sudden vendor bank-account changes
- Spoofed holiday invoices (FedEx/UPS/charities)
- Fake calls from Renasant
- “Fraud is happening right now, you must act immediately” calls

Rule: Pause. Verify. Call back. This solves 80% of cases.

RENASANT | SMITH+HOWARD Advisory LLC

Sample Scripts (What to Say)

If you get a suspicious email:

- Don’t respond to the email, do your due diligence first. (validate sender)
- “I received your request but need to verify it. I’ll call you at the number we have on file.”

If you get a suspicious call:

- “I don’t discuss financial information on inbound calls. I’ll call the bank back directly.”

If a vendor asks to change bank details:

- “We must complete our verification process. Expect a confirmation call.”

RENASANT | SMITH+HOWARD Advisory LLC

Final Takeaways

1. Fraud will make you lose money.
2. Fraud is fast.
3. Fraud is preventable.

Protect your business by following three principles:

Verify → Control → Slow Down

That’s how you break the fraud kill chain.

RENASANT | SMITH+HOWARD Advisory LLC

RENASANT

SMITH+HOWARD
Advisory LLC