

Setting the Backdrop: (Caution & Acknowledgements)

- Don't allow yourself to be shrouded with the "Wet Blanket of Complacency" that too often is thrown on so many – who try to draw out good response/action from our colleagues and managers.
- Every large organization – is more often bridled by flocks of attorneys – that would much prefer us to "not get involved" and certainly "Do not tell anyone" What you are seeing, less we become liable for acknowledging "what we now (already) know".



As many of us continue to look for ways to identify and hopefully defeat globally based cyber threats, altruistically we'd like to believe that most reasonable people would want to do this as well. Sadly, the motivation to actively participate – which usually means sharing critical/timely intelligence (from the Organizations Top to bottom) is not

happening – not because anyone believes it is NOT "The Right Thing To DO" but more often because the organizations we are part of have Mistakenly convinced themselves that:

- There will be some substantial liability risk if we share (Fraud or Cyber Risk/Compromise) details, or
- The positive results of sharing such intel – are not clear and/or convincing, or
- There is not realistic "Downside" or likely repercussions for Not sharing, even if we were to take steps to uncover or otherwise gather such intelligence, that we chose to keep in-house.

We are now in May of 2026, and credible private industry, non-profits like NCFTA, and certain government agencies have worked over the last 10-15 years to correct these misconceptions. Despite these very well catalogued efforts, we continue to find more and more well-meaning (Cross Sector -not Just Banks) Subject Matter Experts (SMEs) that would happily be part of the positive proactive solution (which continues to be urgently needed), but who find themselves bridled or quite literally "Gagged" from participation.

For my view, I still believe that the realistic "Downside" needs to have more substance, if we expect our in-house Legal Counsel participants to release these binds. That, as well as adding enhanced benefits/recognition for active participation should also be further explored.

Moving the ball forward- some Key Points to re-emphasize:

- Information sharing is critical towards both identifying and seeking to neutralize these threats,
- "Responsible" information sharing is what is being sought ie… sharing with known/credible entities (such as the NCFTA or possibly complementary ISAC channels). Remember, getting the best timely intelligence into appropriate Law Enforcement hands – should always be the goal.
- Numerous "Safe-Harbors" protect this activity through: FinCen- SAR Safe Harbors, 314 a & b of The Patriot Act, as well as "Fraud" related provisions of the Bank Secrecy Act (BSA) and more.
- Does anyone really want more Government Audits? Not sure this is the answer, but until now having largely OCC, FinCen (US Treasury Dept), the FCC, FTC as well as the now dismantled CFPB as the primary Government entities overseeing Audits, seems to have fallen short of the desired outcome.

<u>As well-meaning inspired individuals – what can we do?</u>

- Keep turning over rocks, and pointing out to managers what you are finding, (documenting -even informally-will help keep managements attention.
- Keep networking with other like-minded individuals across industries – who are seeing similar/related activities,
- Stat connected/get connected to "working groups" pulling like minded SMEs together,
    - Ensure those working groups have credible "active" participation from Federal (and hopefully international) Law Enforcement (L.E). State & Locals are great to have on board as well – *but Federal L.E will need to help with the ever-expanding footprint tied to Cyber Criminals*.
    - Ensure those working groups are actively looking to expand key SME participation.
- Don't stand by under the often preferred "Wet Blanket of Complacency" , and continue to pose the question – up the line "Is this what you want me to (not) do?
- Remember and remind others:
    - Bad guys continue to evolve and they move fast,
    - Bad guys don't have "lanes" or "AORs" to restrict them,
    - Impact $$ is not just to my company/organization but to the citizens of the US and our Allies -every minute of every day.

I look forward to your participation in this ongoing & righteous fight.