Flashback -to 1998 – "I think we've been here before…"



I recently had a conversation with a former FBI colleague (who is still working there) regarding a request received from a close friend, who was speaking with a recent victim of a (substantial on-line- scheme-from his view) fraud where he lost more than +$180,000 dollars. The victim advised he had filed several complaints with IC3 – as he was guided to – but received no follow up -aside from an automated email. Like many victims, he asked for guidance regarding who he could speak with, and/or if some LE agency would be best for him to reach out to directly.

Upon speaking to my former colleague, I learned that:

1) IC3 did receive his complaints and,

2) His complaint was connected to "a handful" of other similar complaints and that,

3) The aggregate losses were fairly high- but still under $1 million dollars, and also sadly,

4) That No LE agency had yet to show an interest in following up, and

5) Also sadly, that this type of scheme – may not align with "AOR" (Area of Responsibility) priorities for any FBI Field Office.

"Hmmmm – I thought…. This sounds familiar…" (@1998)

I recall – almost like it was yesterday, discussing with FBI Colleagues – as the FBI's Internet Fraud Complaint Center (IFCC) was being announced, how much such a project was truly needed. IFCC would enable consumers to – tell someone (the FBI specifically) about the Fraud Scheme – they were lured into, while also acknowledging why little -or no- attention was given to such matters previously – which included:

- The incident was too small (lower $$ dollar amount) to get Law Enforcement's (L.E) attention (Federal, State and Local included), or
- Victims had no idea which L.E agency to speak to & how to connect to them, or
- The incident involved on-line (Cyber) schemes that most of L.E was not equipped to address (too technical/complex and/or international in scope), or
- On-line fraud schemes were considered "lower priority" as they (at least perception wise) did not involve major Organized Crime or Terrorist tied targets.

This backdrop resulted in many millions of dollars in victim/losses, and hundreds of potential investigations left largely unaddressed ("Circular File material" - which means trash) matters. During it's first two years in existence, the IFCC began connecting hundreds of -previously separated investigations and referred these (further developed intelligence packages) investigations to Federal, State & Local agencies (and some international partners) for follow up. Even in its early days, the IFCC began connecting incidents to larger organized criminal groups (or rings), and in some cases developed connections to groups seeking funding to funnel to terrorist finance organizations.

As 911 came and went, "Fraud" was largely considered (or mischaracterized) as an **even lower priority** for L.E. Recognizing this, the IFCC changed to the Internet Crime Complaint Center (IC3) advising victims to not concern themselves with the "Definitions" of on-line crime, but to just to report these events to the IC3, so that each could be appropriately considered – and connected – to broader criminal conduct – which did indeed merit LE attention.

To aid in this effort, the IC3 substantially ramped up its engagement of key Private Industry partners across multiple sectors – enlisting their substantial intelligence resources (people and data) along the way. Starting in 2002, Private Industry and Academia began providing co-located staff at both the IC3, and the National Cyber Forensics & Training Alliance (NCFTA), which also housed the FBI's High Tech Crimes Task Force in Pittsburgh, Pa.

As the NCFTA Public/Private Alliance model developed, embedded resources from Law Enforcement (LE), private industry (multiple sectors) and academia worked closely together to develop "actionable intelligence" packages where certain substantial organized criminal groups (domestic & international) were identified for further action – usually by LE. In many cases "Best Practices" were also developed along the way, to minimize the likelihood of future exploitation.

As these joint efforts continue to expand, so did the need for additional resources (people and technology). To address the people (analyst & Investigators) part of the equation, cross-sector partners (LE & Industry) expanded their contribution (in kind) and an

expanded Internship program was developed, where academia partners would provide staff to be trained as prospective analysts/investigators.

Exponential Force-Multiplier Resources:

As this process was refined, dozens of analysts-investigators were trained and subsequently hired by the NCFTA and/or cross sector partners (LE, Govt-Intel, & Private Sector) to support this growing collaboration. The successes realized through these efforts, are largely realized and further offered for replication via the "Spheres of Intelligence" project detailed in the next Post, and via "Human Capital Academy" program found at the www.stirtheembers.com website.

(the growing Technology needs were largely addressed via Private Industry partners along the way)