SAMPLE

IDENTITITY SHIELD

INITIATIVE STRATEGY - PLAN

I. Introduction:

The Cyber Initiative and Resource Fusion Unit (CIRFU) and the Internet Crime Complaint Center (IC3) working in partnership with the U.S. Postal Inspection Service (USPIS) and the National Cyber-Forensics and Training Alliance (NCFTA) continue to advance the ID Shield Initiative. Additional Law Enforcement, Industry and U.S Government (Regulatory) agencies are also expected to be included in this initiative. The contributing role of each additional organization will be further defined and incorporated into this plan as they are further clarified. The purpose of this communication is to memorialize the Goals/Objectives of this project, to identify priority intelligence feeds, clarify the daily process flow and triage assignments of supporting staff, and to identity priority threat/actors of the ID Shield Initiative.

II. Goal/Objective:

To expeditiously identify Threat/Actors with ties to the most significant Identity Theft schemes, and to ensure intelligence is collected and developed to an actionable level – in a timely manner – leading to:

1) Subject identification, neutralization

2) Identification of new schemes, tools/techniques worthy of intelligence products, Public Service Announcements (PSA) and/or Anti-Virus (AV)industry notification

3) Victim Mitigation

III. Intelligence Collection (Primary incoming feeds)

Currently, the NCFTA and CIRFU are receiving data feeds from fourteen primary industry partners and Subject-Matter-Expert (SME) groups. The following is a list of these SME/groups and/or data feeds, as well as

corresponding list of NCFTA, CIRFU, IC3 or USPIS responsible staff:

SME/Group – Data Feed	Assigned Staff		
	FBI/USPIS	IC3	NCFTA
ABC Company	SSA Smith/Insp Jones	MPA Simpson	Thompson Schmidt
Bank USA	SSA Ellis/Insp Crabb	TBA	Zang
ISP-Internet	SSA Banks/Insp Lane	Williams	Hennson
DPN –	SSA Smith/Insp Jones	Thornburg Barnes	Wegzyns, Blotter
Financial Services Providers	Eubers, Mulhead, Stromer,	Thornburg Barns	Fishman, Vanlichtenstn, Thomason

In addition to data feeds being received by Industry Partners and SMEs, the CIRFU, USPIS, and NCFTA have a presence on a number of carding forums where consumer data is being stolen, marketed, and sold. Consequently, through such proactive steps, significant additional data/intel is also contributed to this Initiative. All intelligence as well as subsequent analysis/triage efforts will be regularly evaluated against the priority objectives of the initiative, listed above.

IV. Intelligence Triage & Process Flow:

The primary goal of the ID Shield Initiative is to identify,locate and ultimately neutralize the main perpetrators of significant Identity Theft schemes.

- Information obtained from the ID Shield data feeds will be triaged by the respective CIRFU and NCFTA assignees and queried against other NCFTA data in attempt to identify and/or locate subjects, or to connect intel to already known threat/actors.

- After local cross-referencing of intel/data, developed intel packages (reports) will be forwarded to designated IC3 staff for further development against open and closed sources accessible to IC3 staff members. (Incorporating IC3 victim complaint data, interface/de-confliction with FTC and Consumer Sentinel Intel, interface with Social Security Administration, USSS, and other appropriate Law Enforcement or Regulatory

agencies.)

- As existing (potentially overlapping) investigations are identified, designated law enforcement staff will make necessary contact with the identified agency, to clarify the appropriateness of a supplemental referral, and to offer further support if necessary.

- (All such referrals will be coordinated with pertinent substantiveProgram ManagementUnits at FBIHQ)

Another goal of the ID Shield Initiative is to identify new tools or techniques, including malware and zero-day exploits that are being used to further advance Identity Theft schemes. These tools or techniques will be analyzed with the results being reported in the form of PSA's, Intelligence Reports, or samples of malware being provide to CERT/CC and the AV Companies. Intelligence of this nature will also be fed into the NCFTA recently developed MALWARE/CRIME Ware initiative as well.

The third goal of the ID Shield Initiative is Victim Mitigation. Over the last six months the NCFTA has identified over 60,000 compromised credit cards, and thousands of other compromised financial accounts. A procedure has been established, that when compromised accounts are identified they are sent, by the NCFTA, to a central internal email address, catalogued, and sent to the victim institutions, and the credit bureaus for victim mitigation.(CIRFU,USPIS,NCFTA and/or IC3 as appropriate will ensure that the most secure method of transfer (ie encrypted e-mail or similar mechanism)will be utilized to transfer such data.)

Victim Mitigation process flow includes:

- SME Intel feeds routed to “NCFTA.phish” drop folder, or other designated internally accessible-secure location.

- Assigned NCFTA, USPIS, CIRFU staff reviews/analyzes intel for potential overlaps with prior received intel.

- As “Drop” accounts are identified, assigned L.E staff generates “Preservation Request” to identified ISPs and catalogues same.

- Affected financial institution/CC Issuer and credit bureaus notified of compromised accounts – notification catalogued.

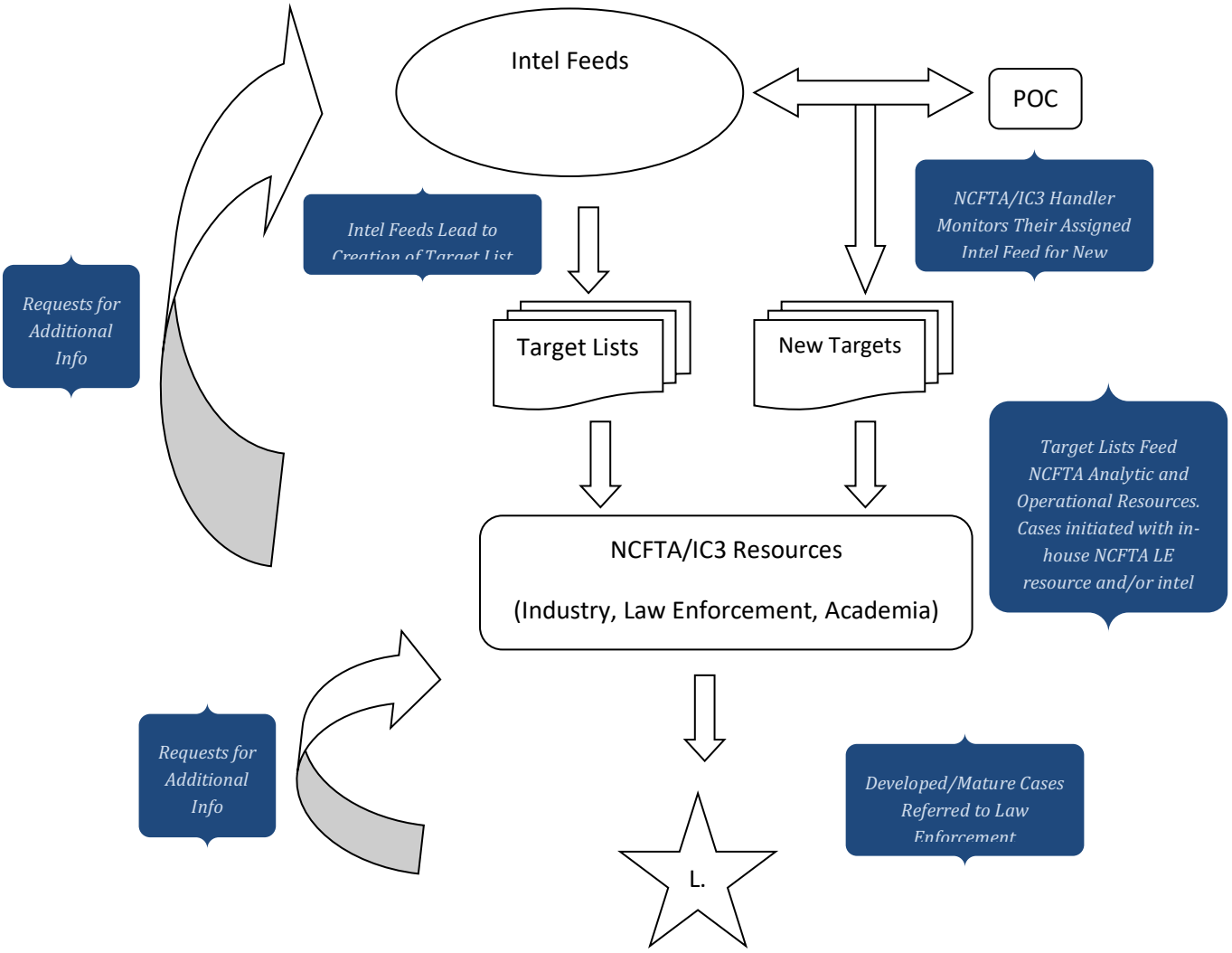
V. Priority Threat/Actors:

Based on current intelligence and SME input, a list ofcurrently identified priority Threat/Actors for the ID Shield includes:

note: It is expected that this table will continue to grow/change as additional top level threat actors are identified, and as assigned resources change, and as identified "gaps" are addressed.

Target Focus	NCFTA/CIRFU Resources	Intelligence Collection (Primary Feeds)	On-going Law Enforcement Case
Bad-Guy Co BP Hosting	Eubers	Super Cops	FBI – WF, RH
	Mckiller	APNGG	
	Zielmanak	Digital Phishnet	
	Hennory	Anti-S	
	Vonlichtenstein	CyFAST	
	Molers		
	Fishstein		
Significance: *Bad Guy Co is a rogue ISP which has hosted sites linked to all manner of Cyber criminal activity. These sites include verified child pornography, phishing, spam, and fraud. This network was home base for the infamous Rock Phish phishing scam.*			
Outside Suites BP Hosting & Malware	Millar	Anti-S	FBI-LA, SE USPIS-AT
	Schummburg	Forums	
	Grilled		
	Marvinson		
Significance: *Significant subject/group in the On-line forum/underground*			
Abd-Dabba BP Hosting	Zooman	You-defend	FBI- TBA DOJ-CCIPS USPIS-TBA USSS-TBA
	Vonlichtenschtein	Supper-Watchman	
	Byerstorm	Forums	
	Salada	Anti-Spam	
	Henson	SpamFlow	
	Yohman		
	McKiller		
	Millar		
	Schummer		
	Griller		
	Fishhead		
Significance:*Abd-dabbaa provides bullet proof hosting for phishing and malware infection/C&C sites. A number of malicious sites that were previously hosted on RBN have migrated to AbdAllah networks. AbbDabba owns servers in various countries such Turkey, Ukraine, and United States and is known as a premier bullet proof hoster within many underground criminal forums.*			

VI. Process Flow (see next page)



1) Incoming **Intel Feeds** stored in designated NCFTA drop folder.

2) **Target Lists** are developed from analysis of Intel Feeds.

3) NCFTA/IC3 Handler(s) (**POC**) monitor their assigned Intel Feeds for **New Targets** and new information relevant to the existing Target Lists.

4) **NCFTA/IC3Resources** analyze information from Intel feeds and develop Intel on specific targets. This results in the development of Intel products that are disseminated to a.) Law Enforcement in the form of case referrals, b.) Industry in the form of alerts and advisories, and c.) Financial Institutions in the form of Victim Mitigation notices.

5) NCFTA staff makes requests for additional information back to Intel Feeds as they develop and refine intelligence on specific targets.

6) Law Enforcement and other Customers make requests to NCFTA for additional information as needed.