Fraud and Theft Opportunities

Opportunities to improve how the industry manages blocklisting

Steve Schwed , Verizon Fraud Strategy

October 4, 2023

About the Speaker …

Steve Schwed

Vice President | CFCA

Verizon | Fraud Strategy Manager

Steve began his career in telecommunications in 1997 with Bell Atlantic Mobile in their Customer Financial Services group before assuming responsibility for the Executive Relations group for the Philadelphia Region in 2000 followed by managing the Verizon Wireless National Executive Relations Team from 2005 until 2013.

In addition, Steve was responsible for maintaining the relationship and service level commitments for responses to consumer complaints for the various Attorneys General, The FCC and other regulatory and consumer advocacy groups.

Steve's involvement with Telecommunications Fraud began in 2013 while working as a Process Manager in the VZW Customer Service Groupand was tasked with addressing issues related to Loss and Policy. Steve officially joined Verizon's Fraud Strategy Team in 2015. He is a member of various GSMA Forums and member of the CFCA and co-chairs the CFCA Handset Trafficking Taskforce.

Steve holds a bachelor's degree in Economics and speaks frequently regarding handset Fraud Losses .

Verizon confidential and proprietary. Unauthorized disclosure, reproduction or other use prohibited.

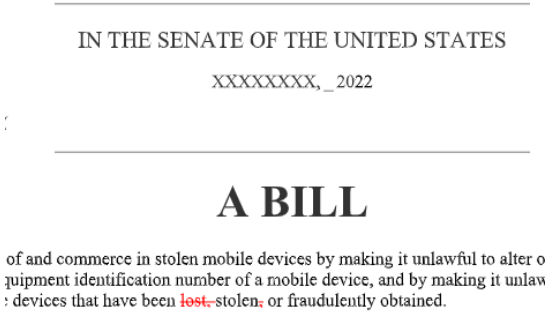
Abbreviated Discussion Points

Blocklist penetration in the Industry and use of the Reason Codes

Brief Discussion on US Carrier Participation in 2022 and the need to expand the number of participants to include OEMs as well as more carriers to make the process more effective

IMEI Hardening

Continue previous industry discussions on what could be done to prevent not only IMEI Obfuscation but improve the ability of OEMs to potentially reduce counterfeit device production



IN THE SENATE OF THE UNITED STATES

XXXXXXXX, _ 2022

A BILL

of and commerce in stolen mobile devices by making it unlawful to alter o
quipment identification number of a mobile device, and by making it unlaw
devices that have been ~~lost,~~ stolen~~,~~ or fraudulently obtained.

US Stolen Phone Legislation CTIA Stolen Phone Working Group.

Update on the current ongoing work with the CTIA SPWG to create meaningful Laws in the US to prevent offering services such as removing devices from the Negative lists, IMEI overwriters and SIM cover import and distribution along with advertising for these services.

Verizon confidential and proprietary. Unauthorized disclosure, reproduction or other use prohibited.

US Carriers are not using the Blocklist Reason codes consistently, allowing certain restricted devices “On Network”

Since inception of the Fraud Reason Code in 2018 , not all carriers were using “Fraudulently Obtained” or the more recent “Court Ordered” reason codes , nor did they appear to be blocking the listings …. Until recently

Results from 2022 the GSMA Annual Report on Blocklisting showed the following data:

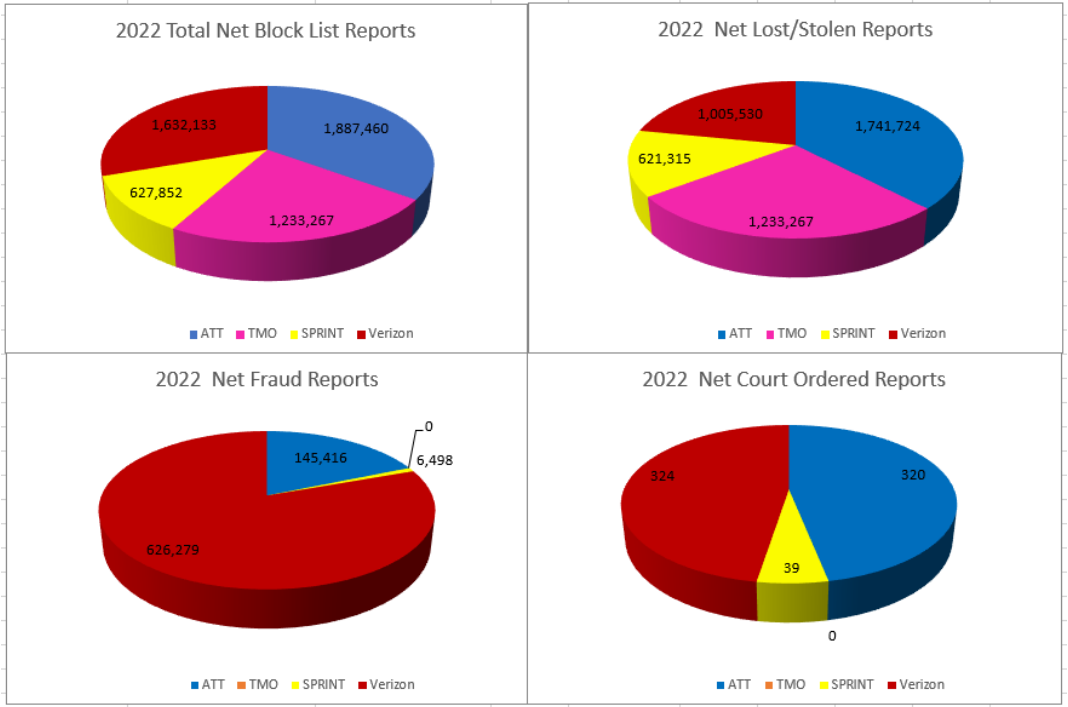
	Stolen / Lost	Fraudulently Obtained	Court Ordered
	11,14	26,27	28,29
AT&T	Yes	Yes	Yes
T Mobile	Yes	No	No
Sprint (TMO)	Yes	Yes	Yes
Verizon	Yes	Yes	Yes

Increased use of the Lost and Stolen Reason Codes was believed to be due to lack of carrier participation than in Fraud codes outside of US – Greater alignment is needed to properly report consumer theft numbers

Greater alignment by carriers GLOBALLY is needed to improve consistency

Verizon confidential and proprietary. Unauthorized disclosure, reproduction or other use prohibited.

The visual and the questions ….



- Are carriers properly identifying the hallmarks of Synthetic ID Fraud ?
- Are carriers not acknowledging Fraud Losses (reporting or subscribing to fraud being reported by other carriers)?
- What can be done to attain greater alignment in the US and Foreign markets?
- If greater participation doesn't occur, will carriers participate with greater scrutiny of their partners?
- Will OEMs start to look at the Fraud Reason code for Bricking devices (Non consumer)

Verizon confidential and proprietary. Unauthorized disclosure, reproduction or other use prohibited.

Are OEMs and the Industry working to solve for IMEI Hardening or are they stymied for a solution?

Recent arrests in Money Laundering Cases (Not device trafficking or stolen device possession) in the US has provided insights that IMEI manipulation and replacement is occurring and organized criminals are attempting to prevent detection of stolen and fraudulently obtained devices.

abc13 EYEWITNESS NEWS

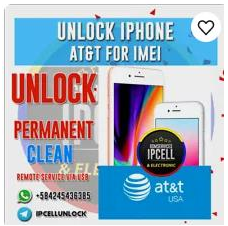
MONEY LAUNDERING

$1.8M worth of stolen devices found in organized crime ring bust in Houston area, investigators say

HOUSTON, Texas (KTRK) -- Three people are under arrest in connection to a $65 million organized crime and money laundering scheme that has fueled many recent cellphone robberies and thefts in the Houston area, investigators said.

Investigators shared that IMEI over writers were found and used in the Houston Operation of "We Buy Phones" .

Hardening or Protecting an IMEI would not only prevent IMEI Obfuscation but could also prevent the counterfeiting of devices

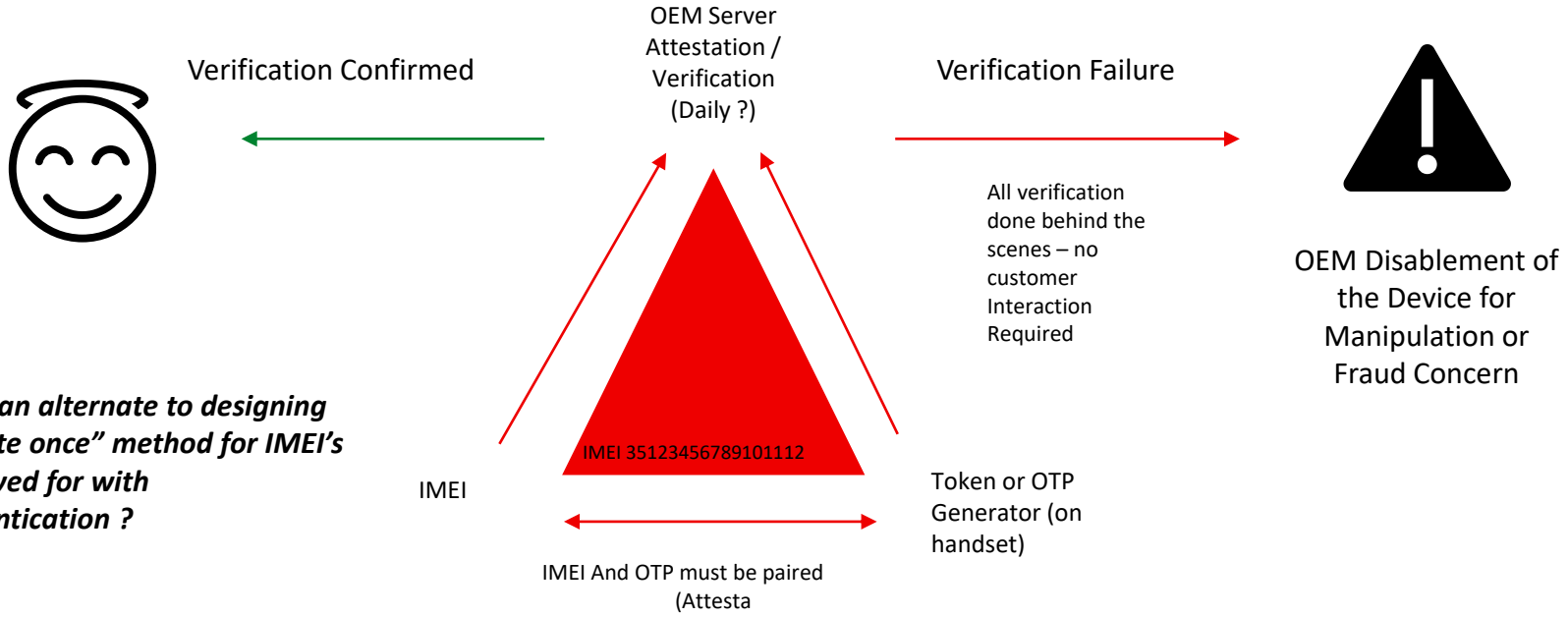


Making it harder to hide the identity of a device will make it easier to prosecute criminals

Verizon confidential and proprietary. Unauthorized disclosure, reproduction or other use prohibited.

How might we harden an IMEI?

What an IMEI Solution incorporating attestation via a Security Token (or One Time Password) specific for the IMEI might look like :



Could an alternate to designing a "write once" method for IMEI's be solved for with Authentication ?

Without duplicating the Token Generator to match the OEM server exactly, counterfeiting could be substantially reduced

Verizon confidential and proprietary. Unauthorized disclosure, reproduction or other use prohibited.

US Stolen Phone Legislation

Work began in 2020 by the CTIA Stolen Phone Working Group to try and update the latest version of the US Code to implement the "Stop Stolen Mobile Device Trafficking Act"

- **Numerous Sessions with Senator Chuck Schumer's office have been supportive, but have yet to yield a formal introduction to the US Senate- (there is still work to do)**
- **Act looks to restrict the advertising, distribution and sale of equipment or services designed to:**
  - Alter an IMEI or any other method of changing the network performance of the Handset ()Such as a SIM lock or Blocklist listing
  - Sale, Import or distribution of devices to alter an IMEI or how a SIM operates
  - Creates a punishable offense for advertising for sale or purchase "Blocklisted" devices and for the trafficking of device lost to theft or fraud

Challenges :

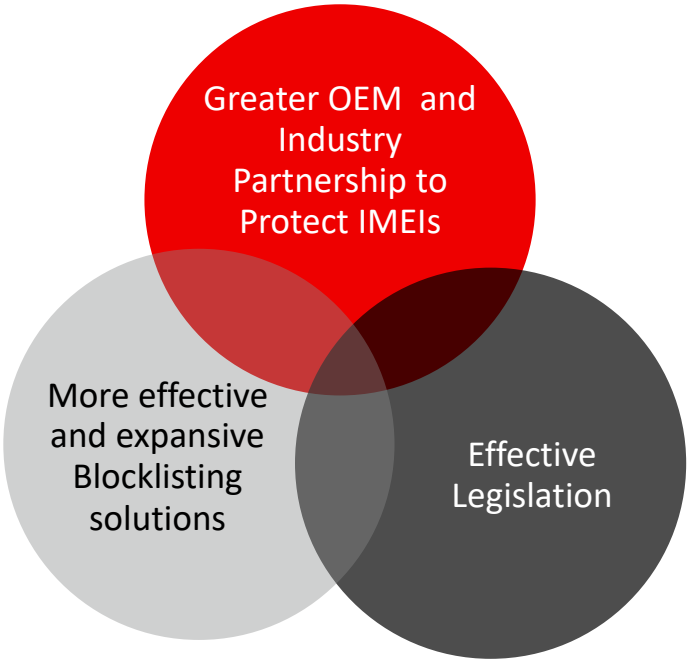
- Multiple delays due to COVID and COVID related legislative efforts
- Varying definitions of Fraud from Country to Country
- Stalemate with Right to Repair Lobbyists

Verizon confidential and proprietary. Unauthorized disclosure, reproduction or other use prohibited.

In summary…

There is no single solution to solve for fraud

- We need to look at enhanced implementation of the blocklists
- Respond faster to fraud strategy of the bad actors
- Continue to pressure regulators and legislators as to the true challenges and question the Status Quo
  - Update the Laws (US -written over 10 years ago)
  - Partner with the proper legislators to advance legislation
  - Expand the legislation to other countries
- Update technology to make sharing block data more cost effective and inviting to smaller carriers



Verizon confidential and proprietary. Unauthorized disclosure, reproduction or other use prohibited.