

-----  
**From:** Harold Chanin[SMTP:HARLENE51@COMCAST.NET]

**Sent:** Friday, May 29, 2015 11:01:40 AM

**To:** PRESS

**Subject:** Financial Cybersecurity

**Auto forwarded by a Rule**

Dear IPTF:

Congressional studies indicate American taxpayers are paying \$200-\$300 billion/year (~10% of federal and states budgets) due to electronic financial theft (EFT) and waste, while American merchants and consumers are paying \$50-\$80 billion/year.

There are two obstacles preventing the prevention of this cyber crime:

1. The Administration has no set policy that each federal agency and department which owns an EFT-enabling system design (e.g.; Social Security, Medicare, Medicaid, Insurance, ACA, Taxes/Rebates, Smart and SmartPay Cards) must remove the theft-enabling ID factor from these electronic financial process (e.g., Social Security/Medicare Cards). The plethora of Congressional ID-Fraud Prevention Committees and Presidential ID-Fraud Prevention Task Forces attest to this technological

failure-to-prevent.

2. Due to international agreement, nobody in the US has authority to do so for commercial payment cards systems designs (e.g.; Credit, Debit, ATM and Chip).

The only known entity which indirectly agrees with these observations is the PTO by granting IP protection for this new cyber technology (No. US 7,991,695 B2 Aug. 2, 2011) which still has not been exploited by these systems designs owners (e.g.; ISO/IEC, SSA, HHS, DOL and IRS).

With no known exception, though each high-ranking official in the Administration is aware of the US cyber technology (replaced EFT-enabling electrons with humans) their sole focus has been on the many limitations of the inventor and none on the potential merits of the US utility invention for EFT-Prevention.

This is also exemplified by those who drafted President Obama's October 17, 2014 EO to help market the costly European microprocessor chip card (e.g., the UK "chip-and-PIN" brand name) which protects from some forms of commercial EFT, but which by design cannot prevent the crime (i.e., net-neutral electrons, not accountable humans, still conduct the critical functions of identity confirmation and authorization to transfer money ownership).

Since Telephone "lines" and Internet "tubes" cannot transfer currency, thus this international crime syndicate's need for human money mules. This is the same engineering principle that while a bullet-proof vest protects its wearer the vest cannot prevent the weapon from firing.

Until President Obama under-takes this needed leadership (i.e., to his related \$1 trillion/year EFT estimate) and to meanwhile move forward, perhaps NIST will coordinate with PTO to pressure ANSI to permit ISO's Secretariat to have S&Es objectively assess the potential merits of this US claim.

Please advise. Thank you.

Sincerely,

Harold Chanin  
President/Engineer

*Cyber-Theft Prevention Associates*  
7811 Lando Avenue  
Boynton Beach, Florida 33437-6359  
(Phones: 561-317-7152, 561-738-2424)