WRITTEN TESTIMONY
OF
Matthew O'Neill

Co-Founder – 5OH Consulting LLC
United States Secret Service (Retired – Deputy Special Agent in Charge - Cyber)

BEFORE

Committee on House Administration
United State House of Representatives

ON

"American Confidence in Elections: Prohibiting Foreign Interference."

December 18, 2024
Washington, DC

Introduction

Good morning, Chairman Steil, Ranking Member Morelle, and distinguished Members of this Committee. Thank you for the opportunity to address the pressing challenge of foreign interference in U.S. elections through money laundering and financial crimes. The topic of today's hearing—"American Confidence in Elections: Prohibiting Foreign Interference"—underscores the urgent need for a coordinated response to safeguard our democracy. Combating these threats requires modernizing regulatory frameworks, leveraging advanced technology, and fostering collaboration across the public and private sectors.

Foreign dollars interfering in U.S. elections pose a profound threat to national security and the integrity of democratic processes. Tackling this issue requires employing the same tools used to combat money laundering and terror financing, such as robust information-sharing systems and closing systemic gaps. By strengthening these mechanisms, we can address not only election interference but also a broad spectrum of financial and cyber threats.

Providing safe harbors for telecommunications companies, ISPs, social media platforms, email providers, domain registrars, and others, to share information, and pairing that with incentives for financial institutions to participate beyond their legally mandated obligations. These changes made in recognition of advancing technology will go a very long way to overcoming the rapidly widening gap between law enforcement and the expanding successes associated with bad actors. These steps will result in a major and fast leap forward toward creating a unified and secure framework for sharing critical information while preserving privacy. Addressing vulnerabilities in one area inherently strengthens protections across all sectors.

While the United States was once a global leader in combating financial crime through landmark legislation like the Bank Secrecy Act (BSA) and the USA PATRIOT Act, it has struggled to adapt to the rapidly evolving global marketplace and technological advancements. Other countries have recognized these shifts and are actively implementing new legislative and regulatory frameworks to address emerging threats.

Today, the U.S. is no longer viewed as a proactive leader in this fight. Global partners, who once looked to the U.S. for leadership, are increasingly forging their own paths, focusing on modernized information-sharing frameworks and advanced technological solutions. The U.S.'s failure to address critical gaps in information sharing and to incentivize collaboration among financial institutions, technology providers, and law enforcement has allowed bad actors to exploit these weaknesses.

This inability to modernize not only diminishes the U.S.'s global standing but also directly harms its citizens by enabling the expansion of illicit activities, including money laundering, fraud, and election interference. Without decisive action, the United States risks falling further behind in its ability to protect its financial system, its democratic institutions, and its citizens from these threats.

The Role of the Secret Service in Combating Money Laundering and Financial Crimes

As a retired second-generation U.S. Secret Service agent, I hold immense pride in the agency's integrated mission of investigation and protection. For nearly 50 years, my family has been deeply committed to uncovering financial crimes and safeguarding national security. Ours is a family of patriots united by a common goal: to make this country safer and better for all.

During my tenure as Deputy Special Agent in Charge of Cyber Operations, I led global investigations into transnational organized crime groups, spearheading initiatives in cryptocurrency tracing, ransomware disruption, and critical infrastructure protection. Under my leadership, the Secret Service expanded its cryptocurrency analysis capabilities by 300% and seized $60 million in illicit assets in a single year. These accomplishments underscore the indispensable role of proactive, technology-driven investigative efforts in combating sophisticated threats.

The investigative mission of the U.S. Secret Service, established 159 years ago, remains foundational to its identity and success. The agency's 43 Cyber Fraud Task Forces, deployed worldwide, are staffed with federal, state, and local law enforcement officers who collaborate to combat complex cyber-enabled fraud. This collaboration has been instrumental in addressing a 200% increase in cyber fraud losses, which surged from $4 billion in 2017 to over $12 billion in 2023, as reported by the FBI's Internet Crime Complaint Center (IC3).

During the pandemic alone, the Secret Service recovered more than $2 billion in stolen funds. Additionally, from FY2019 to FY2023, the agency seized and returned over $687 million to victims of financial crimes, further demonstrating its effectiveness in combating large-scale fraud.

The Secret Service has a long history of success in combating cybercrime and financial fraud. It played a pivotal role in dismantling ransomware networks, including identifying and disrupting the infrastructures behind AlphV and Hive. The agency also investigated the 2020 Twitter hack, where high-profile accounts of political figures were breached. Investigative efforts linked the perpetrator to prior cryptocurrency fraud cases, exemplifying the synergy between the agency's expertise in cybercrime and fraud investigations. Additionally, the Secret Service has disrupted darknet platforms soliciting cryptocurrency donations for targeted violence against elected officials, emphasizing its critical role in mitigating threats to national security.

Since retiring, I have continued to work with government agencies and the financial sector to combat transnational organized crime groups and money laundering. The broader perspective I've received during this time by working with the public and private sectors has only reinforced in my mind the necessity for increased collaboration between public and private entities to counter financial crime and protect democratic institutions.

The Growing Threat of Financial Fraud and Cybercrime
Financial crime has become a global epidemic. In 2023, the Federal Trade Commission's Consumer Sentinel Network reported over 5.39 million consumer complaints, including more than 2.5 million fraud reports, resulting in $10 billion in losses—a record high. Imposter scams alone accounted for $2.7 billion in losses, while investment-related fraud totaled $4.6 billion. The median loss across all fraud reports was $500, with investment fraud yielding median losses as high as $7,768.

Globally, an estimated $2 trillion is laundered annually, representing 2–5% of global GDP. These staggering losses fuel transnational organized crime (TOC) groups, nation-state actors, and other malign entities, jeopardizing economic stability and national security.

Bad actors exploit every available payment system, from open-loop gift cards to cryptocurrency, to obscure illicit funds. Open-loop gift cards are particularly attractive due to their anonymity and ease of transfer, making them a preferred tool for laundering proceeds.

Cryptocurrencies provide another layer of concealment, enabling seamless cross-border transfers with minimal oversight.

According to industry leaders like Cloudburst Technologies, platforms like Telegram have emerged as key hubs for money laundering through gift card exchanges. Fraudsters advertise U.S. gift cards from companies such as Amazon, Walmart, and Roblox in public forums, accepting cryptocurrency in return. These schemes allow bad actors to "wash" illicit funds and reintegrate them into legitimate financial systems.

Modernizing and Enhancing Regulatory and Financial Institution Frameworks
The technology sector, including social media platforms, ISPs, telecom companies, and hosting providers, plays a crucial role in addressing these challenges. However, their ability to act is constrained by liability concerns and a lack of regulatory clarity.

Expanding safe harbor protections akin to those under Section 314(b) of the USA PATRIOT Act to the technology sector would empower these entities to share critical information without fear of legal repercussions. Failure to do will be akin to casting a blind eye to the impacts the fast-growing technological landscape is having around the globe. And explicitly recognizing the intersection of fraud and money laundering by unequivocally extending these protections to be inclusive of those activities would significantly enhance the identification and disruption of criminal networks.

There is also an urgent need to incentivize financial institutions to fully leverage the existing 314(b) framework. Although regulations permit information sharing to combat money laundering, participation among eligible financial institutions remains inconsistent.

Financial institutions often hesitate to collaborate due to competing priorities and perceived risks. Providing incentives such as tax breaks, grants, or reduced regulatory scrutiny for active participants could overcome the voluntary nature of 314(b) and transform it into a cornerstone of the fight against financial crime. Enhanced guidance and feedback mechanisms from regulators would further encourage participation and ensure that collaborations are impactful and compliant with privacy laws.

Sections 314(a) and 314(b) are critical tools in combating financial crime but urgently require updates to address evolving threats.

Section 314(a) enables law enforcement to query financial institutions about accounts or transactions linked to suspected money laundering or terrorism financing. However, the current system relies on, among other things, outdated batch processing methods, delaying responses to urgent queries by up to 28 days. These delays, coupled with an insecure and inefficient information-sharing process based on 22-year-old technology with no substantial updates, significantly reduces the effectiveness of this vital tool.

To address these shortcomings, Congress must fund FinCEN to implement real-time, automated query systems and federated search capabilities. These upgrades are not only technologically feasible but also long overdue. Implementing these improvements will enable law enforcement to detect and disrupt illicit activities with greater efficiency and precision, ensuring a timely and effective response to emerging threats.

Section 314(b) facilitates voluntary information-sharing among financial institutions to detect suspicious activity. However, participation remains inconsistent due to liability concerns and ambiguities in permissible sharing. As noted above, expanding safe harbor protections to include digital platforms, such as social media companies, ISPs, and domain registrars, would empower these entities to share threat intelligence without fear of legal repercussions.

Clarifying these ambiguities, particularly concerning fraudulent activities, would further enhance collaboration and foster a more holistic approach to combating financial crime.

Addressing Inefficiencies in Information Sharing

Siloed information-sharing practices and defensive Suspicious Activity Report (SAR) filings create inefficiencies that hinder the fight against financial crime. Financial institutions regularly file SARs out of caution, overwhelming law enforcement with low-value reports that dilute investigative focus.

Improving feedback mechanisms and reducing the volume of defensive SARs would dramatically enhance their utility. Financial institutions rarely know if their SAR filings lead to investigations or add value. Developing a robust feedback system would help calibrate monitoring systems, streamline reporting processes, and ensure that SARs align with investigative priorities.

Leveraging Advanced Technologies
Technological advancements have widened the gap between law enforcement's ability to detect and deter illicit activities and bad actors' exploitation of systemic vulnerabilities. Criminals leverage sophisticated technology while law enforcement operates within the constraints of a regulatory framework implemented over two decades ago.

Advancements in artificial intelligence (AI) exacerbate these challenges. AI-powered tools like deepfakes, generative text, and synthetic identities lower the barrier of entry for bad actors, enabling even low-skilled individuals to execute sophisticated fraud schemes. Deloitte projects that business email compromise (BEC) losses could rise to $11.5 billion annually by 2027 due to AI adoption, with synthetic identity fraud potentially costing at least $23 billion by 2030.

Despite these challenges, AI also offers transformative potential when harnessed correctly. Fully homomorphic encryption (FHE), for example, enables secure, privacy-preserving data sharing and analysis, allowing institutions to collaborate without compromising sensitive information. By adopting AI-driven analytics and FHE, financial institutions can identify patterns across massive datasets, enhancing fraud detection and prevention.

Regulatory incentives, such as tax breaks or grants, could accelerate the adoption of these tools, closing gaps in the current system and empowering law enforcement to stay ahead of emerging threats.

Fostering Collaboration Across Sectors
Money mule networks remain a critical enabler of money laundering, facilitating the movement of illicit funds across borders. Disrupting these networks requires enhanced monitoring, stricter controls, and coordinated efforts across industries and jurisdictions.

Emerging payment systems, such as open-loop gift cards and cryptocurrencies, further complicate this landscape. These systems are frequently exploited by bad actors due to their anonymity and ease of transfer. Strengthening oversight and implementing stricter controls will be essential to mitigating their misuse.

Fraud and money laundering are deeply intertwined with foreign interference in elections. Bad actors exploit the same systemic vulnerabilities—gaps in identity verification, payment systems, and information-sharing frameworks—to fund malign activities. Addressing these vulnerabilities will not only reduce fraud but also strengthen the integrity of democratic institutions.

Solving fraud and money laundering is a dual-purpose strategy. By improving identity verification, enhancing payment system monitoring, and fostering cross-industry

collaboration, we can dismantle the networks enabling these threats and protect the democratic processes at the heart of our nation.

Recommendations

To address these challenges, I recommend:

1. **Modernizing Section 314(a):** Fund FinCEN to implement real-time, automated query systems and federated searches.
2. **Expanding Section 314(b):** Extend safe harbor protections to digital platforms and clarify sharing guidelines to align with privacy laws.
3. **Modernizing Identity Systems:** Reduce reliance on Social Security numbers and adopt robust digital authentication technologies.
4. **Adopting Advanced Technologies:** Leverage AI and FHE for privacy-preserving data sharing and enhanced fraud detection.
5. **Providing Regulatory Incentives:** Offer tax breaks, grants, and reduced regulatory scrutiny to encourage participation in information-sharing initiatives.
6. **Targeting Money Mule Networks:** Enhance cross-industry efforts to identify and disrupt laundering hubs.
7. **Strengthening Oversight of Payment Systems:** Implement stricter controls on open-loop gift cards and cryptocurrency transactions.
8. **Improving SAR Feedback Mechanisms:** Develop robust systems to provide financial institutions with actionable feedback on SAR filings

Conclusion

Foreign interference in elections through financial crime poses a direct and ongoing threat to the United States. By modernizing regulatory tools, fostering collaboration across industries, and leveraging advanced technologies, we can effectively combat these vulnerabilities. Addressing fraud and money laundering is not merely a financial priority—it is a national security imperative that demands immediate attention.

Thank you, and I look forward to your questions.