FINANCIAL CRIMES INVESTIGATIONS
Improving public-private collaboration to tackle Illicit Financial Flows on Facebook

Omayra Chuquihuara
Harvard Kennedy School

June 2022

M-RCBG Associate Working Paper Series | No. 189

The views expressed in the M-RCBG Associate Working Paper Series are those of the author(s) and do not necessarily reflect those of the Mossavar-Rahmani Center for Business & Government or of Harvard University. The papers in this series have not undergone formal review and approval; they are presented to elicit feedback and to encourage debate on important public policy challenges. Copyright belongs to the author(s). Papers may be downloaded for personal use only.
FINANCIAL CRIMES INVESTIGATIONS
Improving public-private collaboration to tackle Illicit Financial Flows on Facebook

By Omayra Chuquihuara, Master in Public Policy 2022

Prepared for: United States Secret Service (USSS)
Faculty Advisor: David Eaves, Lecturer in Public Policy
Seminar Leader: John Haigh, Lecturer in Public Policy
About the Author

Omayra Chuquihuara is a Master in Public Policy 2022 at the Harvard Kennedy School concentrating on the intersection of business and government. Her coursework and research include digital government, criminal investigations of illicit financial flows, and tech policy. At Harvard, Omayra serves as president of the Harvard Association of Peruvian Students (HAPS), course assistant for government technology implementation, and orientation leader for incoming MPPs. Prior to HKS, she worked on money laundering prevention at the Financial Intelligence Unit of Peru and led capacity-building project implementation for the Organization of American States. A Lima, Peru native, Omayra has a double B.A. in International Affairs and Latin American studies from The George Washington University.

Acknowledgements

I would like to thank, first of all, the United States Secret Service, and in particular Matthew Noyes, for the opportunity to work on this project and the continued support from the beginning to the culmination of the research. I would also like to thank all the unnamed individuals I was able to interview for my research. Your openness and candidness to discuss a complex and ongoing controversial topic on liability was invaluable.

I would also like to thank my PAE advisor, Professor David Eaves, for his unwavering support and guidance on this and other projects I have embarked on while at HKS, as well as my BGP seminar leader, Professor John Haigh, for his feedback throughout this process. This report was also made possible by the support of the Ash Center for Democratic Governance and Innovation, which’s generosity allowed me to delve deeper into the research and was critical for the development of this research.

I would like to dedicate this work to my fellow MPP classmates graduating in 2022. May our work and effort during a pandemic, our advocacy for our collective and individual mental health, and pushback to institutional barriers at HKS bind us together under mutual appreciation and respect for our resilience. Thank you for the inspiration.
ABBREVIATIONS

BSA: Bank Secrecy Act
CFPB: Consumer Financial Protection Bureau
DEA: Drug Enforcement Administration
DOJ (CCIPS): Department of Justice, Computer Crime and Intellectual Property Section
FATF: Financial Actions Task Force
FBI: Federal Bureau of Investigations
FTC: Federal Trade Commission
FinCEN: Financial Crimes Enforcement Agency
FRB: Federal Reserve Board
HSI (ICE): Homeland Security Investigations, Immigration and Customs Enforcement
IFFs: Illicit Financial Flows
IRS (CI): Internal Revenue Services, Criminal Investigations
LEAs: Law Enforcement Agencies
NCFI: National Computer Forensics Institute
NCFTA: National Cyber-Forensics and Training Alliance
SARS: Suspicious Activity Reports
UNODC: United Nations Office on Drugs and Crime
UNCTAD: United Nations Conference on Trade and Development
USSS (INV): United States Secret Service - Office of Investigations
# EXECUTIVE SUMMARY

# INTRODUCTION

# METHODOLOGY

# BACKGROUND

Understanding Illicit Financial Flows (IFFs) .......................................................... 10
Intersection of Digital Technologies and IFFs .......................................................... 12
Conceptualizing IFFs on social media platforms ..................................................... 13
Role of LEAs on IFFs criminal investigations .......................................................... 14
Role of non-governmental actors on IFFs investigations ........................................... 17
Relevance of IFFs on social media for LEAs .............................................................. 18
The Case for Facebook ................................................................................................. 21
Increasing trends on LEA requests worldwide ......................................................... 22
Tying the two together: IFFs on Facebook ................................................................. 23

## KEY FINDINGS ON EXISTING COLLABORATION

Stakeholder analysis ........................................................................................................ 27
Types of stakeholder collaboration ............................................................................... 28
  Type 1 Process: Facebook Portal for Law Enforcement ............................................. 28
  Type 1 Process: Ad Hoc Collaboration ...................................................................... 30
  Type 2 Process: IC3 Reporting .................................................................................. 31
  Type 3 Process: NCMEC Liaison Process .................................................................. 32
  Type 3 Process: NCFTA and NCFI collaboration ..................................................... 33
Main challenges to collaboration on Illicit Financial Flows investigations ............... 34
  Bureaucratic: Inefficient processes ......................................................................... 34
  Restricted: Limited human and budgetary resources .............................................. 35
  Ambiguous: What to do about the gray area? ......................................................... 36

## POLICY RECOMMENDATIONS

Law Enforcement Agencies ......................................................................................... 38
Facebook ..................................................................................................................... 38
Non-governmental actors ............................................................................................ 39

## ENDNOTES
<table>
<thead>
<tr>
<th>APPENDICES</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>Appendix A: Ethics and Transparency Statement</td>
<td>1</td>
</tr>
<tr>
<td>Appendix B: Stakeholder Engagements</td>
<td>2</td>
</tr>
<tr>
<td>Appendix C: Sample Informational Interview Questions</td>
<td>3</td>
</tr>
<tr>
<td>Appendix D: Bibliography</td>
<td>4</td>
</tr>
</tbody>
</table>
EXECUTIVE SUMMARY

The digital era has created new opportunities for criminals to undertake financial crimes in cyberspace. This is the case for the expansion of Illicit Financial Flows (IFFs) on social media platforms such as Facebook. While the threat of IFFs is not new, the increasing use of social media networks is challenging the status quo of criminal investigations led by the United States Secret Service Office of Investigations (USSS-INV) and its partner Law Enforcement Agencies (LEAs). Investigations have shed light to the fact that criminals are using social media platforms to perpetrate IFFs through all three pillars of the chain: earn, transfer, and use. Whether anonymously or not, criminals are able to recruit targeted victims, transfer money, and flaunt purchased goods with illegal proceeds all in one same digital space.

This report focuses on assessing the existing methods of collaboration between LEAs, Facebook, and third-party groups to provide the USSS with policy recommendations on improving cooperation. While the ongoing debate on regulation is important for social media curation, this report does not focus on the legislative and regulatory stance of the equation but rather on the implementation approach and analyzes the potential avenues for collaboration to enhance existing protocols for criminal investigation success on financial crimes. Given the limited research on the use of social media networks as facilitators of IFFs, this report presents preliminary findings on Facebook specifically, with the aim of scaling the research to other social media platforms in the long run.

In the first section, the author presents a framework to better conceptualize the complexity of IFFs on social media platforms before presenting the case for the research on Facebook per se. Through informational interviews with relevant stakeholders, the report identifies the three types of processes that currently exist for collaboration as well as the main challenges for them: bureaucratic processes, limited human and financial resources, and ambiguous gray area for IFFs on social media platforms. For this research, the insights from the public and private sectors were key for anecdotal cases on investigations and final recommendations.

The policy recommendations, resulting from the proposed framework and subsequent analysis on existing collaboration and barriers to success, focus on three stakeholders: LEAs, Facebook, and non-governmental actors. While this report is intended for use by the USSS-INV, the collaborative nature of its mandate resulted in the need to understand the actions needed from each sub-group. These proposed actions in the policy recommendations section cover initiatives on streamlining processes, improving communications, supporting legislation, adapting to a new understanding of IFFs on social media platforms, among others.
INTRODUCTION

The increase in use of social media networks has both positive and negative impacts on society as a whole. On one hand, Facebook’s goal to “connect the world” through its platform has facilitated communications, strengthened relationships, and increased commerce. On the other hand, the tech giant has been criticized in recent years for the negative impact the content has on user’s mental health, its misuse of user privacy, and its heavy focus on an advertisement-based business model that tracks user data. Aside from the alleged negative impact on users, Facebook has also become a hub for criminal activity in cyberspace given the lack (or -as some may argue- limited) curation of activity by users. Enacting crimes such as money laundering, phishing scams, corruption, etc. is easier in the digital age than it was before. Such is the case for the use of social media platforms, particularly Facebook, as a facilitator for illicit financial flows (IFFs).

The United States Secret Service (USSS) Office of Investigations (INV) has under its mandate to “detect and arrest those that engage in crimes that undermine the integrity of the United States financial and payment systems.” This includes leading investigations on financial crimes in coordination with other Law Enforcement Agencies (LEAs). The responsibilities pertaining to the USSS are codified in per USC 3056(b)(3), making its relationship with other LEAs vital to their work, stating that under the direction of the Secretary of Homeland Security, the entity is “authorized to detect and arrest any person who violated any of the laws of the US relating to” (broadly speaking) fraud or financial crime. The focus of this mandate on collaboration highlights that partnerships with LEAs and non-governmental actors are essential to their core work through secondments, task forces, and ad hoc collaboration.

While the threat of IFFs is not new, the increasing use of social media networks is challenging the status quo of criminal investigations led by the USSS-INV and partner LEAs. Criminals have innovative ways of not only earning the money illicitly through recruitment in an anonymous manner but there is indication that the platform serves as means to transfer money and ultimately to flaunt the goods purchased with illegal proceeds.

Investigations point to key cybercrime hubs that utilize social media platforms to earn, transfer, and use funds, however, collaboration from big tech companies (ie. Facebook, Twitter, etc.) and investigative arm of governments are not up to par with the exponential increase in social media use for these crimes. While Facebook’s popularity is decreasing with the rise of other social media platforms such as TikTok and Instagram, it remains the most used online social network worldwide with roughly 2.91 billion monthly active users as of Q4 in 2021.
There is limited research on the use of social media networks as enablers of IFFs. This has translated into little knowledge on how to tackle the new challenges and what this means for collaboration between LEAs and social media companies - particularly in the most ambiguous cases where the crime is not happening on the platform per se. While the ongoing debate on the regulatory front is salient and important, this report aims to provide insight on the implementation approach and analyze the potential avenues for collaboration to enhance existing protocols for criminal investigation success on financial crimes.
METHODOLOGY

For the purpose of this report, the author used primarily two methods of data collection: literature review and interviews with relevant actors. The former includes an in-depth review of academic sources on IFFs, financial crimes, and criminal investigation. Further, the author attempted to review literature on criminal activity on social media platforms, however given that the trends and use as a facilitator is relatively new, academic research is limited. Therefore, on the social media platform side, the author relied on articles, journals, and books on anecdotal information that, combined with information taken from the Facebook Transparency Portal, was able to support the research.

Prior to moving onto the interviews with relevant actors, the author focused primarily on understanding the relationship between the LEAs that deal with financial crimes as well as other private sector and NGO actors that would be helpful in the data collection. Once the primary list was developed, the author coordinated with the USSS-INV who made the connections possible in most instances. In the cases where no direct communication with relevant interviewees was possible, LinkedIn served as a primary means to request interviews and to better understand the relationships between LEAs and Facebook. The initial interviews for this report were held remotely due to the COVID-19 pandemic and subsequently were moved to in-person in Washington, DC, given that the USSS Headquarters and Facebook policy teams are housed there. Finally, a predetermined list of interview questions (Appendix B) with pertinent questions was drafted prior to beginning this phase of the research, yet candid questions were added as a result of anecdotal information provided by the interviewees.

The main piece of missing information from the research was qualitative data gathered through interviews with current employees of the Federal Bureau of Investigations (FBI). While insight was provided by former employees, the information provided by other LEAs and Facebook pertaining to challenges in collaboration was not possible to corroborate. The author mainly focused on the public information found on the IC3 website and public FBI reports. Furthermore, while conversations with current and past Facebook employees were possible, they were limited in number and more content than the publicly-available reports was not provided.

Ideally, this research would also have a quantitative analysis. Yet, due to the confidentiality of criminal investigations and the lack of transparency on criminal activity on social media platforms, quantitative analysis was not feasible. Assessing the correlation between the increased use of social media platforms in recent years and the increase in financial crimes would have been helpful to frame the need to pose the research question to begin with. The novelty of this academic research and the lack of
well-developed frameworks on this intersection was limiting. However, it poses a great starting point for further transparency and research.

Finally, reliance on qualitative data has flaws related to biases from both public and private sector employees. Interviews rely on appreciation of procedures, memory of key examples by interviewees, as well as limitations as a result of privacy concerns. Criminal investigations can pose safety and security concerns to interviewees whether due to the procedure in itself or the employees concern for their involvement in light of their employer. Hence interviewees opted to maintain their anonymity when providing informative insight for this report.
BACKGROUND

Understanding Illicit Financial Flows (IFFs)

Illicit Financial Flows (IFFs) refer to money “illegally earned, transferred or used across borders.” This is an umbrella term that has resulted in debate over whether there needs to be differentiation between funds obtained illegally through criminal activity and flows that are obtained legally but then are used for illegal practices when transferred or used. The former includes proceeds that come from crimes (human trafficking, illicit mining, or drug trafficking as examples of preceding crimes), money that is laundered, and corruption, while the rest refer to legal activities that, for example, fail to pay taxes and thus become illicit (See Figure 1). According to the World Bank, there are three categories that IFFs can be separated into: the acts themselves are illegal; the funds are the result of illegal acts; and the funds are used for illegal purposes. Figure 1 illustrates the differences between IFFs proceeding from legal activities and those from illegal ones.

FIGURE 1

Categories of activities that may generate IFFs

Source: Author's adaptation of IFFs Conceptual Framework by UNODC and UNCTAD
The ongoing debate on the definition of IFFs has resulted in confusion on its difference from money laundering (ML). Money laundering is, by definition, the processing of criminal proceeds to disguise their illegal origin through placing, layering, and, finally, integrating the proceeds.\textsuperscript{xvii} It is a chain that needs to include the three stages in order to be considered ML (Figure 3). These two concepts are oftentimes used interchangeably, despite the fact that the former can derive from both legal and illegal activities while the latter only comes from illicit activity. IFFs can be licit or illicit, the importance is that the flow converts the money to the detriment of the economy and citizens.
ML cannot occur in a vacuum. It has to be connected necessarily to one of the three aspects of IFFs, regardless of whether it happens transnationally or domestically. For this, understanding the intersection of the two spectrums is necessary in order to tackle the complexities in the system and overcome the ambiguity that has created the debate on the definition of both IFFs and ML.

Intersection of Digital Technologies and IFFs

The development of digital technologies has changed the landscape dramatically across the globe. According to Europol, traditional criminal groups have been using digital technologies to enact crime as early as 2014 through a Crime-as-a-Service (CaaS) business model. Further, in recent years, criminals have moved away from the underground digital technologies and are now utilizing public communication networks as facilitators of IFFs - including for ML practices. This is presenting challenges in LEAs ability to tackle these crimes given that responsibility and thus accountability for what takes place in cyberspace is not clear. While the regulatory frameworks for cybercrimes are in place both through hard and soft law in the United States and through international standards, the implementation of the aforementioned is not as clear cut due to the ambiguity that these new technologies bring.

The World Development Report on Digital Dividends sheds light on the intersection of digital technologies and IFFs by cross-referencing examples on the three pillars and then connecting them to the ML chain. The author then provides examples of how these flows can be facilitated through digital technologies. Table 1 demonstrates these intersections in a simplified manner. On the IFFs earn pillar, the source of the income can be either legal or illegal. This means that the proceeds can either be converted to illegal proceeds through tax evasion or they can be illegal from the beginning through criminal activity. In the transfer, whether the money is legal or illegal is not important as it is processed to enter the financial system through placement (Figure 3 Step 1) and through layering (Figure 3 Step 2). Finally, in the use pillar, the money which has already been laundered is re-integrated (Figure 3 Step 3) into the economy through legal means by purchases of goods and investments.
### Table 1
**Intersection of Digital Technologies and Illicit Financial Flows**

<table>
<thead>
<tr>
<th>IFFs</th>
<th>Earn</th>
<th>Transfer</th>
<th>Use</th>
</tr>
</thead>
<tbody>
<tr>
<td>Relation to ML</td>
<td>Source: legal or illegal (ML or no ML)</td>
<td>Process: Placement or layering (ML)</td>
<td>Integration: Re-entering of laundered assets (ML)</td>
</tr>
<tr>
<td>Example</td>
<td></td>
<td>2. Digital/crypto currency</td>
<td>2. Terrorist financing</td>
</tr>
<tr>
<td></td>
<td></td>
<td>3. Online gambling/online betting</td>
<td></td>
</tr>
</tbody>
</table>

*Source: Adaptation of World Development Report on Digital Dividends (2016)*

Up until the increase in use of digital technologies and the innovations surrounding the possibilities of technology, IFF and ML typologies were more straightforward. Take an ML example: a criminal sells drugs internationally to earn a living (Pillar 1), transfers (Pillar 2) the money by placing it into the financial system and then layers said proceeds, finally the criminal uses the proceeds (Pillar 3) to purchase a car with the proceeds, thus integrating the laundered assets into the financial system. The changing landscape and increased use of digital technologies prompts us to rethink existing frameworks and pushes society to better understand the importance of social media curation to tackle said crimes.

**Conceptualizing IFFs on social media platforms**

The development of digital technologies has led to the use of information and communications networks as a tool for facilitating IFF. Within this realm of digital technologies fall communication networks such as social media platforms. These platforms have become a key challenge to tackle the problem as following the money trail of illicit funds has become harder. On top of this, the transnational component in the definition of IFFs has become more complex in social media platforms seeing that while a company may be based in a specific country, the users could be all over the globe. This presents problems not only in the existing definition, research, and typologies but also in the legal processes that hold companies accountable and the existing collaboration mechanisms between LEAs of different countries.

Given the lack of consensus over the term IFFs and the ongoing debate of whether tax evasion should be included, the author of this report proposes a new framework to
understand how these are present on social media platforms. To begin, the framework maintains both the notion of the three pillars, incorporates money laundering into two of the pillars, and works under the assumption that the cross-border component of IFFs is met given that borders in cyberspace are fluid. The key difference between the framework proposed in Tables 1 and 2 is on the “use” pillar, for which the latter proposes a differentiation in relation to ML and incorporates the integration of money in cyberspace as a portion of the transfer pillar and replaces it with flaunting the money through social media networks.

**TABLE 2**

**IFFs on social media**

<table>
<thead>
<tr>
<th>IFF</th>
<th>Earn</th>
<th>Transfer</th>
<th>Use</th>
</tr>
</thead>
<tbody>
<tr>
<td>Relation to ML</td>
<td>Source: legal or illegal (ML or no ML)</td>
<td>Process: Placement or layering (ML) / Integration: Re-entering of laundered assets (ML)</td>
<td>No ML</td>
</tr>
<tr>
<td>Social Media</td>
<td>1. Criminal activity on social media:</td>
<td>1. Financial transactions through a marketplace</td>
<td>Using and/or flaunting of money on social media once assets have been purchased offline (ie. car purchases, house expansions, bitcoin, investments, etc.)</td>
</tr>
<tr>
<td>Examples by pillar</td>
<td>phishing, scamming, etc.</td>
<td>2. Financial transactions on the platform between users directly</td>
<td></td>
</tr>
<tr>
<td></td>
<td>2. Communications to enact criminal</td>
<td>3. Cryptocurrency transactions</td>
<td></td>
</tr>
<tr>
<td></td>
<td>activity on the platform or through other</td>
<td>4. Terrorist financing on platform</td>
<td></td>
</tr>
<tr>
<td></td>
<td>portals.</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

*Gray referenced in text depicted in coloring

Source: Author’s creation derived from the World Development Report on Digital Dividends (2016)

**Role of LEAs on IFFs criminal investigations**

The landscape of LEAs that deal with IFFs is complex. There is a need to understand the wide array of actors for this report given the approach to collaboration inherent in the USSS’ mandate per USC 3056(b)(3), as mentioned above. Its relationship with the National Computer Forensics Institute (NCFI) and approach to Cyber Crime Task Forces on a federal and local level with both public and non-governmental actors demonstrates the variety of types of collaboration and the potential for improvements - the main objective of this report’s recommendations.
There are international as well as national actors that deal with all three pillars shown in Figure 2, but for the purpose of this research on collaboration, national actors are center stage with limited reference to international entities that set international standards. Briefly, the international actors that set standards for anti-money laundering (AML) and tax evasion and have or will be mentioned throughout the report primarily for definition-purposes are: the Financial Action Task Force (FATF), the United Nations Office on Drugs and Crime (UNODC), and the United Nations Conference on Trade and Development (UNCTAD).

This section will detail on a high level the relevant actors to IFFs prevention and investigation, however, a stakeholder analysis on the actors grouped together that can implement the recommendations of this report is available in the “Key Findings.”

Going back to Figure 1, since IFFs include both legal and illegal activity as part of the chain, the scope of LEAs includes all the agencies relevant to money laundering both on a preventive and investigative capacity as well as those relevant to tax financial crimes. This includes all preventive, supervisory, regulatory, and punitive law enforcement actors that at times overlap in mandates and responsibilities.

According to the Mutual Evaluation Report on ML led by the FATF for the US, the federal LEAs that have principal investigative authority on financial crimes in an identification or analysis phase are: the Drug Enforcement Administration (DEA), the FBI (Federal Bureau of Investigation), HSI-ICE (Homeland Security Investigations - Immigration and Customs Enforcement), IRS-CI (Internal Revenue Service - Criminal Investigations), and USSS. Aside from the investigative arm, the following supervisory entities are also important to IFFs prevention: FinCEN (Financial Crimes Enforcement Agency), the Federal Trade Commission - Criminal Liaison Unit (FTC) and IRS-CI. In terms of punitive measures, the Criminal Division of the DOJ (DOJ-CRM) houses relevant actors that deal with IFFs, such as the Fraud Section, the Computer Crime and Intellectual Property Section (CCIPS), the Money Laundering and Asset Recovery Section, among others. This division within the DOJ, along with line public prosecutors in the U.S. Attorney offices that deal with specific cases, work with other LEAs to tackle IFFs. Further explanation of the competencies of a few of these relevant actors are detailed in the following paragraphs.

FinCEN, a bureau of the US Department of Treasury, is tasked with administering the anti-money laundering and counter-terrorist financing law on a federal level, including the Bank Secrecy Act (BSA) that is relevant to regulatory entities. This entity has the authority to issue regulations implementing the BSA, examine financial institutions for compliance, and take enforcement actions for violation of the BSA. FinCEN also oversees
certain institutions directly and supervisory entities that are tasked with supervising in turn other institutions (such as the financial supervisor).\textsuperscript{xxvii} Given that there are a variety of competent authorities on all government levels that use financial intelligence such as Suspicious Activity Reports (SARs) to lead investigation and prevention utilizing different private databases depending on their operational needs, as well as identify risks, FinCEN is tasked with supervising their collaboration.\textsuperscript{xxviii}

In line with the work led by FinCEN related to the BSA, the Federal Financial Institutions Examination Council (FFIEC) promotes uniformity of the supervision of financial institutions and provides a BSA/AML Examination Manual as guidance for financial institutions and their supervisors.\textsuperscript{xxix} Under this group, a final key actor for IFFs prevention is the Consumer Financial Protection Bureau. Another example of collaborative task forces that deal with financial crimes is the President’s Working Group on Financial Markets (PWG) which is chaired by the Secretary of the Treasury and consists of representatives from the Federal Reserve, the Securities and Exchange Commission, and the Commodity Futures Trading Commission.\textsuperscript{x} These different groups represent a few of the existing collaborations that are committed to preventing and mitigating financial crimes as set in national and international standards.

The FBI, through its criminal investigations on cyberthreats as well as on white-collar crime, is a key player for IFFs prevention and detection. In terms of cyber threat, the FBI is the “lead federal agency for investigating cyberattacks and intrusions” and works to engage victims and share intelligence to pursue criminal investigations.\textsuperscript{xxxii} In terms of the white-collar crime work, the FBI pursues investigations on criminal activities that include aspects of the IFFs change such as public corruption, money laundering, and a wide variety of fraud and identity theft from different actors on a national, regional or international level.\textsuperscript{xxxiii} Furthermore, the FBI is currently spearheading the initiative for the US Administration to combat virtual currency misuse to launder ransom payments as a part of the Ongoing Public US Efforts to Counter Ransomware.\textsuperscript{xxxiv} Their active role in prevention of virtual currency misuse shows its central role in financial crime prevention as expected for the future.

An important tool that has proven to be valuable in engaging civil society as well as in tracking typologies and trends is the Internet Crime Complaint Center (IC3) - an arm of the FBI. The mission of the IC3 is to provide the “public with a reliable and convenient reporting mechanism to submit information to the FBI concerning suspected Internet-facilitated criminal activity, and to develop effective alliances with industry partners.”\textsuperscript{xxxv} The IC3 reports break down the number and typologies of complaints received on their website, demonstrating how the landscape has changed throughout time since its first report in 2004.
The FTC’s Criminal Liaison unit civil enforcement actions “support prosecutors to increase the number of criminal consumer fraud cases and get restitution for consumers or disgorgement to the US Treasury.”\(^{xxxvi}\) Additionally, the FTC gathers “reports from consumers about problems they experience in the marketplace” and stores them in the Consumer Sentinel Network (Sentinel), identifying fraud, identity theft, among other topics.\(^{xxxvii}\) This secure online database is available only to law enforcement and while the FTC does not intervene in disputes, its LEAs partners nationally and internationally use the information to identify typologies. To make its work easier, in 2020, the FTC launched the ReportGraud.ftc.gov platform which reduces costs associated with reporting and encourages consumers to submit reports that can be shared with more than 3,000 law enforcers.\(^{xxxviii}\) The platform is very clear about the fact that the FTC is not able to ultimately resolve the complaint but that, through collaboration, investigations and cases can be opened.

On a local level, state regulators and agencies also play an important role in coordinating with federal agencies on financial crimes. For example, the Departments of financial services in New York\(^{xxxix}\) or in Florida\(^{xl}\) not only receive alerts on fraud but also provide information on financial literacy in order to prevent scams that can result in criminal activity. Increasingly, police agents are using social media to fight crime\(^{xli}\), increasing the need for them to be an important stakeholder in the conversation of financial crimes on Facebook. Their role is primarily important for the relationship with non-governmental actors in investigations.

**Role of non-governmental actors on IFFs investigations**

Aside from the main two types of stakeholders for collaboration on financial crime investigations for the purpose of this report (LEAs and social media platforms), there are relevant third-party collaborators that are essential in supporting interactions between the public and private sectors. The two main collaborators identified in this space are the National Computer Forensics Institute (NCFI) and the National Cyber-Forensic Training Alliance (NCFTA).

The NCFI is a federally funded training institute that has under its mandate to “train and equip state, local, tribal, and territorial (SLTT) law enforcement officers, prosecutors, and judges” in digital evidence and cybercrime investigations.\(^{xlii}\) Since its creation in 2008, NCFI has partnered with law enforcement agencies to tackle a variety of cybercrimes given the new challenges to law enforcement through digital technologies that threaten critical infrastructures.\(^{xlii}\) This initiative is key as, despite being reliant on federal funding, the trainings are focused on local LEAs tackling challenges that are specific to smaller jurisdictions that do not have as much human and financial resources as larger ones.
It is important to note for the rest of this research that the NCFI is currently undergoing revision as its current mandate to educate and train SLTT has a timeline from 2017 through 2022.\textsuperscript{xlv} The partnerships with LEAs and private sector actors, the specific activities to be carried out by NCFI as well as its budget are being revised, hence it is an important opportunity to envision its role as a key stakeholder in the collaboration for financial criminal investigations.

The NCFTA, unlike the NCFI, is a nonprofit partnership between private, public, and academic sectors to serve as a neutral entity that enables "collaboration and cooperation to identify, mitigate and disrupt cybercrime."\textsuperscript{xlv} Since its creation in 1997, the NCFTA has been perceived as an international model for collaboration between LEAs, private sector, and academia to stop and mitigate cyber threats.\textsuperscript{xlvi} The information exchange of intelligence and the free flow of information among partners is key, according to the head of the Cyber Initiative and Resource Fusion Unit (CIRFU) assigned to the NCFTA. The collaboration includes secondments between law enforcement agencies and partnerships to share aggregated data that helps in cybercrime prevention and monitoring. The secondments and liaisons between entities work together to facilitate conversations and thus information sharing between private sector and law enforcement. While the information on their successes in promoting collaboration is publicly available on their website, their notoriety in this space is not large as gathered throughout this research.

These two stakeholders, while important players in the cybercrime prevention space, are small when compared to the number of crimes in the past decade. Therefore, this report takes them into account as key stakeholders in the potential for increased collaboration as facilitators of conversations and information sharing.

**Relevance of IFFs on social media for LEAs**

Financial crimes occur on a multitude of platforms. The importance of regulating or supervising financial transactions is not new and the prevention systems to tackle financial crimes are -in many cases- robust. However, the landscape continues to change, and such is the case with the increasing reliance on digital technologies.

The Mutual Evaluation Report (MER) published by FATF, reports that the US conducts a large number of financial investigations that result in over 1,200 money laundering convictions on average at the federal level per year.\textsuperscript{xlvii} This only considers Pillar 2 in the IFFs chain in which money laundering takes place, yet it does not take into consideration the number of investigations that are -or could- be derived from the earn or use pillars. The potential that goes unnoticed or underreported is vast.
Aside from the importance from a money laundering investigation and prevention perspective, the amount of suspected Internet-facilitated criminal activity affects people on a daily basis. The IC3 reports that in the last five years, there have been a total of 2+ million complaints through its website with an average daily of over 2,000 complaints received by the office. The latest report from 2020 states that internet crimes related to phishing, vishing, smishing, pharming (important for the earn pillar) had a total of 241,342 victims as financial crimes and that 35,439 of these victims fell to the criminal activity through social media platforms, including Facebook.

Comparing the statistics on this type of financial crime, the IC3 reports that in 2018 the victim count was 26,379, which means that in two years the number of victims is approximately ten times higher in this type of financial crime. In terms of financial loss, $155,000,000+ happened on social media, presenting an important number of the total reported through the platform. Therefore, whether through victim count or financial loss, social media and financial crimes as reported by the IC3 are considerable. This merits more attention from LEAs on the necessary collaboration from social media platforms in general to tackle internet-based crimes as reported by users.

The FTC’s Consumer Sentinel serves as an investigative cyber tool for the members of its network by providing them with access to reports that aggregate data on a variety of threats to consumers, including identity theft. This network is free of charge and available on all levels of government, through federal, state or local law enforcement agencies. In 2021, the Consumer Sentinel Network received over 5.7 million reports in the US from consumers, including 2.8 million in fraud (close to half of the reports), 1.4 million in identity theft, and 1.5 million in other types of reports. Of the fraud reports, approximately 25% reported that money was lost, surmounting to $5.8 billion lost to fraud which increased by $2.4 billion over the reported statistics in 2020. According to the breakdown of contact methods of fraud reports, social media was the second highest contact method of fraud that resulted in dollar loss reported, despite being 5th in terms of contact method after phone calls, texts, e-mail, and websites (See Figure 4).
The increasing trend is relevant for all stakeholders that deal with IFFs. In the case of the NCFTA, when the non-profit was created, the biggest threat according to the FBI was spam to users, however the organization now deals with malicious viruses and other financial frauds by organized crime groups. According to the FBI and the FTC, cybercriminals are attempting to steal people's identities and personal data to commit fraud and this typology of crimes is only increasing. This is the case of a targeted fake ad that advertised high salaries for shuttle drivers when in reality it was collecting people's personal data to file unemployment insurance claims. Similarly, every day cases of identity theft or fraud schemes through social media continue to arise, such as for example the case of a national operation from Massachusetts that attempted to steal social media accounts and cryptocurrencies. To date, there are hundreds if not thousands of cases like these both available publicly online or that have been identified throughout interviews for this report.

Source: FTC's Consumer Sentinel Report 2021
The Case for Facebook

While there are a variety of social media platforms nowadays that could have been assessed for this report, the fact that Facebook continues to have one of the highest numbers of users in the world makes it a good starting point for this research which - in the long-run - could be scaled to other platforms.

The main concern from a collaboration standpoint is whose responsibility it is to tackle IFFs on the platform given the overlapping mandates and recent debate between privacy of users and security of users. Facebook’s portal states that the company is “committed to making Facebook a safe place (by removing) content that could contribute to a risk of harm to the physical security of persons” while also being “committed to protecting personal privacy and information.”

Taking the example of the collaboration between the US National Center for Missing and Exploited Children (NCMEC) - which will be elaborated upon in the following section - the proposed changes in privacy policies in 2019 raised concerns about the tracking and availability of data that could be used in criminal investigations. These changes sparked debate particularly given that in 2018 Facebook submitted 16.8 million reports to NCMEC which represented more than 90% of the total reports that year. With these changes, NCMEC estimated that 70% of Facebook’s reporting would be lost.

These changes in privacy policies present a concern given the potential information that is lost when reconciling the privacy and security mandates Facebook has under its community standards and policies. On one hand, as a society, there has been a shift towards criticizing social media platforms due to weak standards to protect user’s information. On the other, the information that is scraped from both public and private sources is valuable in order to track criminal activity on the platform. While society wants privacy of their data, they also believe that platforms like Facebook have a responsibility to support LEA with criminal investigations.

This debate, and concern for surveillance, is not only from users towards the private sector but rather a concern for citizens from a public-sector LEAs perspective as well. As a result of a request for an investigation from US Senator Ron Wyden (D-Oregon), DHS-HSI put a stop to a surveillance program of money transfers that were happening between Southwest US and Mexico, calling for transparency and consistency with US law. According to Wyden, LEAs have authority to follow legal processes to gather financial information and thus using resources to collect millions of transactions jeopardizes individuals’ privacy.
In the case of IFFs on Facebook, the fact that the crime is not necessarily happening on the platform (aside from the IFFs transfer pillar) makes the considerations on privacy and security even more complex. The increasing use of social media platforms, the increasing trends on LEA requests, and the debate on privacy vs. security is drawing more attention to the roles and responsibilities on each side of the spectrum. The societal shift towards demand for “moral responsibility” of the private sector to support the public sector - not only on criminal investigations - is resulting in legal obligations and changing supervision. Their commitment to safety must not only be on paper through its community standards and policies but rather through an alignment and true commitment to prevent non-violent crimes on its platform.

Increasing trends on LEA requests worldwide

Currently, data from the Facebook transparency portal shows an exponential increase across the world from law enforcement agencies requesting information to access user data both through normal legal processes as well as through expedited means (ie. with no legal process in cases of emergency). This is particularly the case in the US, as shown in Figures 5 and 6. Given the increasing trend, better understanding the challenges to collaboration that is effective and efficient to prevent these crimes is needed. The subsequent sections of this report aim to analyze through the information gathered in interviews whether the existing mechanisms (ie. through the law enforcement portal, Mutual Legal Assistance Treaties, and other types of collaboration) are sufficient to tackle the increasing demand.

FIGURE 5

![U.S. LEA Requests Received by Facebook](image)
Tying the two together: IFFs on Facebook

The lack of consensus on the definition of IFFs and the complexity of ML makes understanding IFFs on social media platforms equally confusing. For this, going back to Table 2 is helpful, where the three pillars are accompanied by broad examples of what each would look like on social media.

However, delving into one specific example and tying it to how LEAs tackle the regulation and supervision will provide clarity on the argument for better collaboration. This section takes an imaginary example case derived from anecdotal evidence from the interviews held throughout this research.

<table>
<thead>
<tr>
<th>TABLE 3</th>
<th>Explanatory case of IFFs on Facebook</th>
</tr>
</thead>
<tbody>
<tr>
<td>Pillar 1 (Earn)</td>
<td>The criminal targets vulnerable individuals on a Facebook Group that is meant and advertised for finding job opportunities for unemployed US citizens in a particular area. The criminal reaches out via Facebook Messenger and creates a relationship with the individual. Ultimately, the criminal gains the individual's trust and either continues the communication via Facebook Messenger or via WhatsApp (where it is encrypted). While there is no crime happening on the platform, thus part of the gray area, it is the breeding ground for criminal activity and the hub for Pillar 2.</td>
</tr>
</tbody>
</table>
Pillar 2 (Transfer) | The criminal, in an effort to launder money from illicit proceedings, after gaining the initial trust, requests that the targeted individual transfer X amount of funds through Facebook Pay (with a maximum of $9,999 as permitted on the platform) to a third person, criminal Y, and the criminal will provide the money in cash or via alternative means that will make the transaction between the criminal and person Y seem like autonomous transactions. This creates separation between criminals thus making the money trail harder to trace.

Pillar 3 (Use) | Criminal Y, once the funds are received, uses the money to purchase goods and through layering posts photos on Facebook flaunting the goods purchased or the travel that they acquired. While there is no crime happening on the platform since the illegal proceeds are not being used on the platform, thus part of the gray area, it is linked to illicit activity and makes it part of the chain as stated in sections above.

Therefore, the role of LEAs and other collaborators to tackle the three pillars on Facebook is essential. Supervising and collaborating on Pillars 1 and 3 is more complex than in Pillar 2 given the gray area component where crime is not being committed on the platform per se. For this, an explanation of the role of LEAs in the pillars is necessary.

To comply with regulations and collaborate with LEAs on Pillar 2, Facebook has registered two Money Service Businesses (MSB) with FinCEN which are required to report transactions: Facebook Pay, Inc. and Calibra, Inc. Calibra, however, is not being utilized given the pushback it received from users and law enforcement and from the general public. There is also a digital wallet that Facebook has launched, Novi - however, this report will not delve into this space.

The FATF, in its MER, as well as the US under its National Risk Assessment of 2016 identified as key vulnerabilities to the AML regime the following: cash, banking, MSB, casino and securities sector. The BSA and overall AML prevention regime requires financial institutions to file either Suspicious Activity Reports (SAR) as well as Currency Transaction Reports (CTR) depending on the type of transaction in order to prevent financial crimes from taking place. The former, SAR, is a standardized document that the financial institution files to FinCEN if they suspect possible money laundering, terrorism or fraud. The latter is additional reporting that the BSA requires financial institutions in accordance with the Department of Treasury’s implementing regulations when a currency transaction exceeds $10,000. If a transaction exceeds both the
threshold and is considered suspicious then both an SAR and a CTR must be submitted to FinCEN.

The main limitation with this approach is the fact that the cap for Facebook Pay, inc. limits the transactions to $9,999 which gives the entity space to determine reporting and relies on their willingness to do so when identifying transactions (See Figure 7). The potential use of Calibra as well as talk of cryptocurrency used on Facebook particularly is also an area of examination on the platform in future research regarding their role in criminal investigations.

![FIGURE 7](Facebook Pay Transaction on Facebook)

The more concerning Pillars as identified in this report are Pillars 1 and 3 given that there is no regulation and legislation that requires Facebook to monitor the activity surrounding criminal activity on the platform - namely, as stated before, the gray zone. While there is a willingness to collaborate with LEAs as shown in the Transparency Portal through the requests posed by the government on a national and international level, there is room for improvement. Currently, there is an push towards moving the approach to financial crime prevention towards an investigator-centered approach\textsuperscript{1} and the teams at Facebook are limited in this front - due to prioritization and business model.

For Pillar 1, the top three messaging applications by number of users are WhatsApp (2 billion users), Facebook Messenger (1.3 billion users), and WeChat (1.12 billion users) with Facebook Messenger being the top messaging app in the US.\textsuperscript{2} Given that Meta owns the first two, the argument for having clear standards on what communications are monitored or not is necessary. This is exacerbated by the use of youth using social media
to enact crime or to learn about it through these platforms.\textsuperscript{lxxv} As people spend more time online and are more interconnected through messaging apps and social media, the windows and opportunities to engage in criminal activity online have also increased.

Similarly, for Pillar 3, in an interconnected world of influencers, vloggers, and users who share their daily endeavors with their follower base, criminals have fallen into the trap of oversharing to the point where illicit activity can be tracked. This was the case of Hush Puppi\textsuperscript{\textit{lxxvi}}, a convicted money launderer who ultimately was caught, among a variety of other indices, by looking at the Instagram page where assets were being flaunted that did not coincide with his earnings.\textsuperscript{lxxvii} Such cases have also been highlighted through interviews with law enforcement agents tasked with scraping social media to find not only communications in Facebook groups (Pillar 1) but also flaunting of goods (Pillar 3) to track money trails and potentially find indices of laundering.

There is vast potential for collaboration between Facebook and LEAs to build robust criminal investigations on IFFs. Or, at the very least, to start them. For this, understanding the existing collaborations - discussed in the next section - is essential prior to creating recommendations on the matter.
KEY FINDINGS ON EXISTING COLLABORATION

Understanding the landscape of existing collaboration was key in order to be able to implement the framework posed in the earlier sections. For this, stakeholders were interviewed to delineate their responsibility in financial crime investigations aside from the purview of their responsibilities under their mandates. While legislation and regulation can specify each actor’s responsibility, in reality, responsibilities fall through the cracks. The following stakeholder analysis aims to present the key stakeholders relevant for this analysis from the private, public, and non-governmental sectors.

Stakeholder analysis

For this report, the stakeholders noted so far in the sections above have been grouped into four different categories to better assess the existing processes of collaboration in the following section. The categories are: (i) LEAs; (ii) social media platforms, (iii) non-governmental actors; and (iv) users as shown in the table below. The four categories group the stakeholders that are relevant for this particular research but should not be taken as all-encompassing for future research, namely for the second subcategory that focuses only on Facebook.

<table>
<thead>
<tr>
<th>Category</th>
<th>Interests</th>
<th>Resources</th>
</tr>
</thead>
<tbody>
<tr>
<td>Law Enforcement Agencies</td>
<td>Ensure safety and security of jurisdictions.</td>
<td>Knowledge on criminal investigation processes.</td>
</tr>
<tr>
<td></td>
<td>Better understanding of what collaboration with social media platforms looks like.</td>
<td>Bottom-up pressure to pass new regulatory legislation for social media companies.</td>
</tr>
<tr>
<td></td>
<td>Automated processes that lessen bureaucracy and increase ability to produce timely investigations.</td>
<td></td>
</tr>
</tbody>
</table>
Types of stakeholder collaboration

Taking the stakeholder analysis, the report presents the five main mechanisms grouped into three different types of processes used by the aforementioned to collaborate and share information in order to make robust criminal investigations. These include existing collaboration between LEAs and the platform per se as well as other engagements between the stakeholders. The stakeholder collaboration noted in this research focuses on LEAs-Facebook (Type 1 Process), Users-LEAs (Type 2 Process), and non-governmental actors-LEAs (Type 3 Process).

Type 1 Process: Facebook Portal for Law Enforcement

The first type of process identified is the formal process through Facebook’s Law Enforcement Portal. Introduced in 2015, it is the primary means of communication from domestic and international LEAs to request information on an account (whether an
individual or a group) from Facebook. To be eligible to use this portal, an official email from a LEA must be provided and the format must be filled out regardless of the type of request. The company reserves the right to turn requests down, including due to lack of appropriate supporting documentation or private concerns as some of the most common examples of limitations.

For the United States, the portal can be used to submit preservation requests as well as all other official requests for records that are part of a criminal investigation. This includes emergency requests, subpoenas, court orders, search warrants, among other investigative support documentation that has necessary information. These U.S. Legal Process Requirements are explicitly shared on the platform’s website and states that the account records can be shared if disclosure is compelled “in accordance with (their) terms of service and applicable law, including the federal Stored Communications Act ("SCA"), 18 U.S.C. Sections 2701-2712.”

The main two challenges that have been identified for domestic requests through the LEA Facebook portal are twofold: (i) lack of understanding of the documentation needed to submit a request - particularly from smaller jurisdictions; and (ii) lack of guidance and clarity on what the process entails once the information request has been submitted. These two can also be attributed to limited human resources on both ends of the collaboration. The fact that the only documentation found on guidelines of how to navigate the portal was created by a Sheriff’s department exemplifies the lack of clarity and need for Facebook to publish an official guidebook for submitting requests.
For international LEAs, while the process is the same, the information that can be provided through the portal is limited. A request can be submitted through the portal by a foreign LEA, however many smaller international jurisdictions are not aware of the limitations of submitting said requests and the mechanisms that must be followed in order to receive account information. International actors must first submit a request through a Mutual Legal Assistance Treaty (MLAT) agreement. When requesting information from Facebook, foreign LEAs must follow the legal process through formal mutual legal assistance. Through this bilateral agreement, LEAs are allowed to use another country's investigative capacities in their own criminal proceedings.

The lack of understanding of this process, however, is exemplified in the number of requests that are received through the portal from international LEAs. Interviewees noted that the requests from some foreign LEAs did not follow the formal process and thus were denied by the company. While Facebook reports the number of requests it receives from LEAs (and, as noted in earlier sections, there has been an exponential increase) as well as the number of requests that produce “some data,” it does not clarify how much data and what the parameters to release data are. Taking the information received from interviewees, the bilateral relationships between the US and other countries is hypothesized to explain the differences in number of requests received through the portal. For example, the Canadian government has requested 2,569 in this past quarter while others remain much lower. The Canadian government uses the MLAT process to request information as well as ad hoc collaboration with the Law Enforcement Response Team (LERT) and Law Enforcement Outreach team, therefore not utilizing the platform to the extent other countries use it for criminal investigations which could ultimately explain the large difference in number of requests with international LEAs.

Type 1 Process: Ad Hoc Collaboration

The second type of collaboration identified under this process is the informal, ad hoc collaboration that stems from one-to-one relationships between Facebook and LEAs. The LERT team and Law Enforcement Outreach team in the US are the primary points of contact with government officials. The former is in charge of processing all the requests through the Facebook portal yet does have direct interaction with government officials while the latter builds the collaboration and is the informal point of contact for LEA agents. The outreach team also is a primary point of contact for emergency requests for which LEAs oftentimes have questions on the turnaround time and/or need immediate assistance with timely requests submitted as “emergency requests” where user endangerment is imminent.
Through informational interviews with Facebook, while the specific number of individuals who work for each of these teams was not clear, it was inferred that the number of employees working on both is not sufficient for the number of requests that they receive. Furthermore, with the recent increase in requests from both domestic and international actors, the projected number of employees should be higher. For the LERT team, there are upward of 150 employees that process requests, including reviewing, requesting more information if needed, and sending the account information along.

The main limitation found in this type of collaboration is the fact that it is heavily constrained on both ends on human resources and, on the LEA side, tied to financial resources that the agency can access to hire more agents. For the outreach team on Facebook’s side, the main limitation is that the collaboration relies heavily on the type of relationship between the entities and the availability and desire of Facebook employees to support ongoing processes. For example, the number of employees on the outreach teams per region within the US and as points of contact for international LEAs is not sufficient for the number of questions that the team receives on how to process requests either through the portal or through the MLAT process.

Furthermore, the incentive from the private sector to continue funneling resources into the LERT and outreach teams is questionable from a business-centric perspective. While part of the Terms and Conditions as well as the data policies on Facebook focus on the safety and security of users, there is a business model that works based on the traction of users on the platform. The traction is created by a multitude of content, including some that could be harmful to users - such as is the example with mental health concerns from bullying that happens on Facebook. While this paper does not focus on the complexity behind the business model and the regulation that has sparked debate over recent years, it is important to note that this also affects the financial and human resources that the company is willing to provide to tackling crimes and actions related to criminal activity such as is the case with the gray area for IFFs.

Type 2 Process: IC3 Reporting

Another type of collaboration on financial crime investigations is focused on user-LEA collaboration that then translates into a civil lawsuit in the majority of cases from Facebook users themselves. This fourth process is through the FBI’s IC3 Reporting portal. This platform gives victims of Internet crimes (including financial crimes occurring in cyberspace) the opportunity to submit an Internet complaint with the IC3 and detail from their experience and voluntarily the following information: (i) financial transaction or attempted financial transaction; (ii) description of the incident; and (iii) information about the subject who victimized the person presenting the claim.
While this platform focuses primarily on the IFFs transfer pillar, the information provided when explaining the case can help LEAs - in this case the FBI - to create a more robust investigation as the victim can present information on the form that is helpful to the earn and use pillars. However, this type of collaboration relies on users themselves to produce the complaint and include the necessary information that could be helpful to LEAs on financial crime investigations. This takes away from the responsibility of the platform to report, primarily on the transfer pillar but as collateral on the earn and use pillars as well. This reliance on the victim creates undue burden on them and removes the responsibility on the platform to collaborate with LEAs when instances related to any of the pillars happen on the platform.

**Type 3 Process: NCMEC Liaison Process**

For the Type 3 process, the first type of collaboration identified through interviews and background research is the liaison mechanism between the National Center for Missing and Exploited Children (NCMEC) and Facebook. Since 2011, the two have collaborated to combat online child sexual exploitation through direct reporting. NCMEC does not need to submit a petition to request information from the platform but rather Facebook proactively sends the information from the scraping of the information that they find.

The figures that have prompted this type of unique collaboration are significant. In 2020 alone, Facebook reported to NCMEC more than 20 million child sexual abuse images - which includes Facebook and Instagram data - more than any other company and more than 35 times as many reports as Google which follows in the ranking. This statistic alone, and the fact that it is a trending increase in the past years, shows the root cause of this collaboration that does not exist with other private sector entities.

The uniqueness of this collaboration can be explained by: (i) the fact that NCMEC is classified as a private, non-profit 501(c)(3) corporation which makes information-sharing from Facebook to the entity easier; and (ii) Facebook's interest and commitment to prioritize the prevention of crimes pertaining to children on its platform. These two aspects are exemplified by the fact that Facebook holds a seat in the Board of Directors of NCMEC and the fact that the company provides one of the highest financial pledges per year to the organization - namely upwards of $1,000,000 along with other corporations.

The limitation to set up such a mechanism for financial crimes on the platform such as the one with NCMEC is mainly the fact that the crime, as shown in Table 2, is not only happening on the platform. These gray areas in which the “earn” and “use” pillars do not
constitute crimes that happen on the platform per se but rather the pre- and post-communications and flaunting makes it harder to establish a NCMEC-style collaborative mechanism since the red flags are not black or white regarding these two pillars unlike in child abuse and exploitation.

Type 3 Process: NCFTA and NCFI collaboration

This process of collaboration is different from the previous ones identified as it focuses on increasing the knowledge and skills of agents who deal with financial crimes in cyberspace. This type of collaboration stems from initiatives both by NCFTA and NCFI through their mandates of promoting private and public sector collaboration. This process, while not a direct collaboration between LEAs and social media companies, helps in making financial crime investigations more robust which is the ultimate objective.

Interviewed subjects from NCFI noted that, to date, there are 18,000+ LEA agents on both a local and federal level in the US who have graduated from one of the digital forensics certificates they provide since the beginning of their offerings in 2008. NCFI’s three tiered approach (first responder, digital forensics, and advanced forensics) teaches agents a wide range of skills, including how to have one-off undercover conversations with individuals in groups on Facebook all the way to identifying patterns and understanding malware that could help in investigations. A key example of this type of initiative is the “Social Networking Investigations” (SNI) which is a course specifically designed for agents who focus on combating cybercrime on social media. This particular course is, at the time of this report, being updated in order to tackle the different levels of knowledge and wide range of sub-topics that could be targeted.

NCFTA takes a different approach to this type of collaboration - primarily focusing on task forces and secondments between agencies in order to increase data collection and data sharing. This entity primarily facilitates interactions to aggregate information and promote information sharing between private sector entities and law enforcement. NCFTA, from 2015 to 2021, by producing actionable intelligence for its partners, has prevented $12.25 billion in financial loss, helped LEAs seize $178 million, and produced 4,184 cases that were referred to law enforcement agencies, among others.

However, while the advances from these initiatives are clear, their scalability so far is limited. The main concern for the collaborations that NCFI and NCFTA have is financial and human resources. While the demand for collaboration in the case of NCFTA continues to increase, more human resources are needed in order to scrape data that is relevant and helpful on both ends of the spectrum. In the case of NCFI, the human resources are mainly a problem given the increasing request for more courses that cover
social media platforms and criminal investigations. The latter is also tied to another limitation: lack of collaboration with social media platforms in order to make the course well-rounded and comprehensive. Finally, per the interviews held, there was a clear concern with the fact that much of the conversation on these collaborations is felt as one-sided. While the aggregated data is coming from both sides of the spectrum, willingness to share red flags or typologies is higher from the public sector. This seems to stem from an understanding of the need to protect the whole ecosystem rather than just the institution. The fact that this is a one-sided conversation for prevention, the understanding of what the private sector needs in order to better collaborate on financial crime prevention on its platform is limited.

Main challenges to collaboration on Illicit Financial Flows investigations

This section describes the three main challenges drawn from the collaboration processes in IFFs criminal investigations developed in the previous section. While each collaboration has its own limitations and advantages as described above, this section aims to highlight the three that are transversal to all processes regardless of the stakeholders involved.

Bureaucratic: Inefficient processes

For the direct collaboration between Facebook and LEAs, the legal request process is cumbersome and lacks clarity. The lack of clarity regarding roles and responsibilities and fragmentation particularly between LEAs given the number of stakeholders weakens the system’s resilience and response capacity which is the case for the global cyber threat to financial systems, as identified by the Carnegie Endowment.

The lack of human interaction on the Facebook portal when submitting a request presents roadblocks for successful submission both from national and international LEAs. On a national level, regular and emergency requests are held up in many cases because of lack of understanding from local LEA agents on the legal supporting documents needed - for smaller jurisdictions given that this is not the case for bigger jurisdictions that are accustomed to submitting requests. The 90 day threshold of responding for requests is therefore longer in order to obtain the necessary information.

Furthermore, while comparatively there is better clarity on the legal processes for submissions from national LEA agents, the MLAT process for international actors within the portal is not clear and therefore requests are still being submitted without the proper supporting documentation. Aside from the lack of clarity, there is general consensus from
stakeholders on the inefficiency of the MLAT process which is outside the scope of this report but is a valuable insight to attempt to change bilateral collaboration between countries to more efficiently deal with criminal investigations.

In terms of user reporting, bureaucracy is again an impediment. Given that for this report, agents from the FBI were not available for interviews, the turnaround time for submissions on the IC3 portal was not obtained. However, from research on public information and through informational interviews, the fact that there is no information on what the process looks like hints at the same or similar challenges identified for the Facebook portal in terms of clarity to ensure quick turnaround time.

Restricted: Limited human and budgetary resources

The increasing requests both nationally and internationally directly from LEAs to Facebook and through reporting on the IC3 website demonstrates the need to increase resources to cover the demand. As noted earlier, the number of employees dealing with collaboration, and namely on financial crimes, in Facebook as well as in LEAs and non-governmental actors is limited. The former mainly due to the way Facebook is set up and the priorities it holds while the latter given financial restrictions that do not allow for hiring on this specific matter.

The information gathered by the Department of Justice on the limited number of law enforcement agents on a federal and state/local level is evident by the lack of updated information that exists through the Bureau of Justice Statistics. In 2016, the Bureau reported that there were approximately 100,000 full-time federal law enforcements in the US that provide police protection and 701,000 in general-purpose state and local law-enforcement agencies. An example of the limitations when compared to the number of investigations is shown in the IRS-CI Report for Fiscal Year 2021 (Figure 9). The fact that 3% of the investigative sources come from state and local government yet the relationship with the NCFI is primarily with training local/state LEAs shows the need to increase the number of employees on this level.
The identification of this concern poses questions when looking into the future. The future of collaboration will depend highly on the resources funneled into these organizations both in the public and private sectors to tackle IFFs. Therefore, the three types of relevant stakeholders (LEAs, Facebook, and non-governmental actors) are subject to overcoming these restrictions to be able to scale their current actions and promote comprehensive collaboration opportunities on criminal investigations.

**Ambiguous: What to do about the gray area?**

This is the most concerning challenge area for collaboration on financial crimes on Facebook. While on paper there is clarity on which entity (within the public and the private sector) is mandated to oversee which pillar on the IFFs chain, in practice the lines are blurred, therefore making it harder to delineate the scope and thus the type of collaboration that must exist. The ambiguity of the lines and the responsibilities of each actor is concerning for the future of collaboration given the increasing use of the platform in all three pillars.

First of all, even the transfer pillar - which should be the clearest cut given its responsibility to report to FinCEN and the IRS and the existing liability if failing to do so - presents challenges. The limit set on Facebook Pay of up to $9,999 per transaction, while seemingly arbitrary, is important to address given the need to report above the $10,000
threshold to FinCEN. There is also increasing concern of the potential move towards encrypted communications on Facebook Messenger which would limit the ability to obtain the information needed for criminal investigations from the platform. The fact that communications can currently be moved to WhatsApp (an encrypted application) and thus all communication lost means that the transfer of money could be happening on a different platform that is closely linked to Facebook without the need for the crime to happen on the platform per se. Additionally, the launch of a beta WhatsApp payment system in certain countries will make the transfer pillar even more complicated to regulate as it creates further spaces to perform criminal activity on different -but related- applications and platforms.

However, the most concerning to date is the ambiguity of the gray area as described in sections above. There is an increasing use of Facebook for the earn and use pillars under the social media framework presented in Table 2. The ambiguity of whether it is Facebook’s responsibility to report actions related to the criminal activity or whether LEAs should request the information as is done until now must be resolved. The lack of a clear delineation of responsibilities for connecting actions to the crime both for international and national standards contributes to the rest of the challenges. Without a clear notion of whose responsibility it is to report and/or track on the earn and use pillar results in lack of appropriate human and financial resources being funneled into the public and private sector teams. This, in turn, creates inefficient collaboration and potential duplication of efforts as well as cracks where criminal activity can take place or be flaunted without supervision.
POLICY RECOMMENDATIONS

The ultimate goal of the research presented is to have a better understanding of the landscape of IFFs in social media platforms - namely on Facebook - to present recommendations that will improve cooperation between entities. Taking the findings a step further, given the collaborative nature of the USSS for financial crime investigations, the policy recommendations have been subdivided into three groups: LEAs, Facebook, and non-governmental actors. The following recommendations correspond to the key findings identified in the section above.

**Law Enforcement Agencies**

**RECOMMENDATION 1:**
Promote among LEAs the re-definition of the role of social media platforms as a reporting entity by expanding to the “earn” and “use” pillars (not sufficient to report under an MSB category for FinCEN through its payment portals).

**RECOMMENDATION 2:**
Determine, with multiple stakeholder engagement, new financial compliance thresholds to report for social media companies as reporting entities to Financial Intelligence Units within the “transfer” pillar.

**RECOMMENDATION 3:**
Draft typologies regarding the three pillars of IFFs on social media platforms so that LEAs and Facebook can better identify pre, during or post criminal activity and supporting entities can reference these as well.

**RECOMMENDATION 4:**
Create a custom FBI-IC3 reporting portal access point for social media platforms (unique log in) to facilitate criminal investigations by streamlining communications.

**RECOMMENDATION 5:**
Reduce fragmentation and avoid duplication of efforts by developing clear engagement protocols, with the goal of reducing transaction and operational costs. This recommendation should occur on a national and international level.

**Facebook**

**RECOMMENDATION 1:**
Mainstream communications with LEAs to decrease ad-hoc collaboration, improve efficiency, and decrease roadblocks to communications (Facebook Portal for LEAs
that include communication options and assigns people to submissions, not solely to submit legal processes).

**RECOMMENDATION 2:**
Promote transparency by tracking data and making criminology/typologies on platform public (overall and specific to financial crimes) rather than showing LEA requests only.

**RECOMMENDATION 3:**
Promote transparency by giving parameters on what constitutes “some” data produced under the LEA requests to Facebook Transparency portal. The increasing percentages on documents produced, while helpful, do not provide insight on what the information looks like and whether it is helpful to entities.

**RECOMMENDATION 4:**
Promote transparency by showing financial and human resources being funneled to tackle crimes by the company.

**RECOMMENDATION 5:**
Increase financial and human resources on Facebook to respond to the increasing number of requests, set specific parameters on the number of cases tackled by each agent per time period to avoid cracks in the system.

**RECOMMENDATION 6:**
Provide clarity on the company’s stance on the alleged contradiction and debate on privacy vs. security of its users. Set clear guidelines so that moral obligations as perceived by its users and LEAs are aligned with legal and reporting obligations.

**Non-governmental actors**

**RECOMMENDATION 1:**
Strengthen the partnership between LEAs and the NCFTA to share information and create more secondments for law enforcement agents

**RECOMMENDATION 2:**
Utilize the 2022 renewal of NCFI under USC 383 to incorporate expressly private-public collaborations with social media companies to “educate, train, and equip” law enforcement agents, including establishing a pathway to receive funding.

**RECOMMENDATION 3:**
Support the creation of the Illicit Virtual Asset Notification (IVAN) led by the FBI to create more information sharing partnerships between LEAs and social media platforms.
ENDNOTES


xiii “Illicit Financial Flows (IFFs).”


xx Tropina, “Do Digital Technologies Facilitate Illicit Financial Flows?”


xxii “18 USC 3056: Powers, Authorities, and Duties of United States Secret Service.”

xxiii The FATF is the international body that creates


“Transparency Reports | Transparency Center.”

“Transparency Reports | Transparency Center.”

FinCEN, “Calibra, Inc. MSB Registration Status Information” (Department of the Treasury, June 2019).


Financial Crimes Enforcement Network, “Questions and Answers - General Information about the MSB Registrant Search Web Page” (Department of the Treasury, n.d.).


Detective James Williams, “The Unofficial Guide to Facebook’s Law Enforcement Portal Version 2” (Sacramento Internet Crimes Against Children Task Force, n.d.).

LEAs, Interview 1, Zoom, January 2022.


“Safety Center.”


Private Sector, Interview 2, In Person, January 2022.

Private Sector.


“IC3 Complaint Referral Form.”


NCFI, Interview 3, Phone, January 2022.


NCFTA, Interview 4, Phone, January 2022.


APPENDICES

Appendix A: Ethics and Transparency Statement

The research and writing for this PAE was primarily conducted using existing reports from think tanks, international organizations, non-governmental actors, the federal government, and state government as well as from original data from interviews held by the author with experts in the field. For data requests, the interviewer and interviewees discussed the need for confidentiality given the nature of the work both private and public sector agents lead as well as the recent scrutiny over regulation in the past years. Much of the evidence in this report is non-attributable and individual names are therefore withheld to protect the privacy of contributors given the potential reputational harm as well as the sensitivity of the topic. Furthermore, the recommendations posed and information drawn could also be controversial causing potential harm to interviewees, thus the need for privacy. For further information on the list of organizations, refer to Appendix B.

This report was granted funding by the Ash Center for Democratic Governance and Innovation which was used to finance travel to conduct the research and meet with the client as well as with public and private sector stakeholders.
Appendix B: Stakeholder Engagements

The list of stakeholder engagements is not exhaustive and it does not include the number of interviews held per institution to maintain as much anonymity to interviewees as possible.

Carnegie Endowment for International Peace  
Facebook (Meta)  
Financial Crimes Enforcement Network (FinCEN)  
Financial Action Task Force (FATF)  
Federal Bureau of Investigations (former agents)  
Harvard Law School  
Harvard Kennedy School  
Harvard Business School  
Harvard College  
National Computer Forensics Institute (NCFI)  
National Cyber-Forensics and Training Alliance (NCFTA)  
Private sector companies on data analytics  
Technology and Public Purpose (TAPP), Belfer Center  
United States Secret Service (USSS)
Appendix C: Sample Informational Interview Questions

This list of questions was created prior to holding interviews and is a preliminary list to obtain basic information from the institutions. Some of them were adjusted previous to each interview and cannot be disclosed for privacy reasons. Other questions were a result of comments made by interviewees and are also not included.

1. What are the trends in recent years that law enforcement has seen in terms of financial crimes in the US? Follow up: What is the role of digital technologies in financial crimes?
2. Is there quantitative data that sheds light on potential correlation between increase in use of social media and increase in use of these mediums to use, transfer or earn said money?
3. What role do private sector companies that analyze trends and investigate crime play in this area?
4. What role do social media platforms play in criminal investigations on financial crimes?
5. How can the private sector support the public sector in dealing with this phenomenon? Is there interest in doing so?
6. Are there differences between using social media platforms in the different areas of the IFFs chain?
7. Is there a specific social media platform that is being used in any of the three pillars of the chain more significantly than others?
8. What potential areas of collaboration exist to tackle IFFs investigations? What are the stakeholders that are involved?
9. How does money laundering differ from IFFs? What is the role with social media platforms?
10. Is there potential for a liaison mandate on supporting law enforcement such as the one with the National Center for Missing and Exploited Children (NCMEC)? What are the limitations?
Appendix D: Bibliography


Broussard, Meredith. “When Cops Check Facebook.” The Atlantic, April 2015.


The Block. “Facebook Announces Its Crypto Subsidiary Calibra Is Registered with US


———. “Questions and Answers - General Information about the MSB Registrant Search Web Page.” Department of the Treasury, n.d.

FinCEN. “Calibra, Inc. MSB Registration Status Information.” Department of the Treasury, June 2019.

———. “Facebook Payments, Inc. MSB Renewal Registration Status Information.”
https://www.fatf-gafi.org/faq/moneylaundering/.
NCFI. Interview 3. Phone, January 2022.
NCFTA. Interview 4. Phone, January 2022.
https://about.facebook.com/technologies/novi/.
https://www.propublica.org/article/scammers-are-using-fake-job-ads-to-steal-peoples-identities?token=YxUntiDH12MOMHz5OD1yLBp1hr4wTzdEG.
Reaves, Brian A. “Census of State and Local Law Enforcement Agencies.” Bureau of Justice Statistics: Department of Justice, July 2011.


