

## HOUSE OF REPRESENTATIVES

DAVID SCHWEIKERT, ARIZONA, CHAIRMAN  
JODEY C. ARRINGTON, TEXAS  
RON ESTES, KANSAS  
LLOYD K. SMUCKER, PENNSYLVANIA  
NICOLE MALLIOTAKIS, NEW YORK  
VICTORIA SPARTZ, INDIANA

DONALD S. BEYER JR., VIRGINIA  
GWEN MOORE, WISCONSIN  
SEAN CASTEN, ILLINOIS  
DAVE MIN, CALIFORNIA

RON DONADO, EXECUTIVE DIRECTOR

## Congress of the United States

JOINT ECONOMIC COMMITTEE  
(CREATED PURSUANT TO SEC. 5(a) OF PUBLIC LAW 304, 79TH CONGRESS)

Washington, DC 20510-6602

## SENATE

ERIC SCHMITT, MISSOURI, VICE CHAIRMAN  
TOM COTTON, ARKANSAS  
TED BUDD, NORTH CAROLINA  
DAVID MCCORMICK, PENNSYLVANIA  
MARSHA BLACKBURN, TENNESSEE  
ASHLEY MOODY, FLORIDA

MARGARET WOOD HASSAN, NEW HAMPSHIRE,  
RANKING MEMBER  
AMY KLOBUCHAR, MINNESOTA  
MARTIN HEINRICH, NEW MEXICO  
MARK KELLY, ARIZONA

LAURA EPSTEIN, DEMOCRATIC STAFF DIRECTOR

December 17, 2025

The Honorable Scott Bessent  
Secretary of the Treasury  
U.S. Department of the Treasury  
1500 Pennsylvania Ave NW  
Washington, DC 20220

Dear Secretary Bessent:

We are writing to request information about the ways in which the Department of the Treasury (Treasury) and U.S. technology companies are engaging to disrupt overseas scam networks and protect Americans from fraud and the foreign adversaries that enflame it, as well as the staff and other resources that the Treasury dedicates to this effort. Last year, overseas scam networks stole an estimated \$10 billion from Americans through sophisticated criminal compounds that are based in Southeast Asia and are often staffed through the forced labor of trafficked workers.<sup>1</sup> These scam compounds often rely on U.S.-based technologies — including social media and online dating platforms, artificial intelligence models, peer-to-peer payment applications, and satellite internet services — to identify, target, and defraud victims. New technology has contributed to the proliferation of these overseas compounds in recent years. Still, “U.S. efforts [to expose and deter this growing threat] remain fragmented and under-resourced,” according to the U.S.-China Economic and Security Review Commission (USCC).<sup>2</sup>

Online scammers overseas routinely use technology or online platforms owned by American companies to defraud victims in the United States. For instance, to begin a scam, criminals frequently initiate contact with potential victims on American-owned social media and online dating platforms. In the first half of 2023, at least half of individuals who reported financial losses from an online romance scam to the Federal Trade Commission (FTC) said that

---

<sup>1</sup> U.S. Department of the Treasury: *U.S. and U.K Take Largest Action Ever Targeting Cybercriminal Networks in Southeast Asia* (Oct. 14, 2025).

<sup>2</sup> U.S.-China Economic and Security Review Commission, *China’s Exploitation of Scam Centers in Southeast Asia* (July 18, 2025) ([www.uscc.gov/sites/default/files/2025-07/Chinas\\_Exploitation\\_of\\_Scam\\_Centers\\_in\\_Southeast\\_Asia.pdf](http://www.uscc.gov/sites/default/files/2025-07/Chinas_Exploitation_of_Scam_Centers_in_Southeast_Asia.pdf)).

the scam began on a social media platform.<sup>3</sup> Similarly, a co-owner of one popular peer-to-peer payment application notes that nearly half of the scams that its consumers report originate on social media.<sup>4</sup> In addition, more than half of online dating users believe that they have encountered a scam.<sup>5</sup> Scammers can also lend credibility to their communications with the use of artificial intelligence models developed and owned by American companies. In a February 2025 report, for example, one leading artificial intelligence company noted that scammers in Cambodia had used its technology to generate personalized English-language messages and sustain conversations with users on social media.<sup>6</sup> Once they gain a victim's trust, overseas scammers then solicit payments through American-owned peer-to-peer payment apps, where transfers are instant and, as the FTC notes, difficult to reverse.<sup>7</sup> Finally, as an official from the U.S. Secret Service testified to Congress, scam compounds in Southeast Asia are increasingly turning to American-owned satellite internet service for the connectivity that often makes these online scams possible.<sup>8</sup>

Moreover, scam compounds in Southeast Asia reportedly operate with the tacit approval of Chinese state actors as part of a symbiotic relationship built on the exploitation of others.<sup>9</sup> As described in the USCC report on these networks, criminal actors like Chinese crime boss Wan Kuok-Koi ("Broken Tooth") have reinvented themselves into pro-CCP businesspeople as they

---

<sup>3</sup> Federal Trade Commission, *Social Media: A Golden Goose for Scammers* ([www.ftc.gov/news-events/data-visualizations/data-spotlight/2023/10/social-media-golden-goose-scammers](http://www.ftc.gov/news-events/data-visualizations/data-spotlight/2023/10/social-media-golden-goose-scammers)) (accessed Aug. 13, 2025).

<sup>4</sup> Chase, *Alert: For Your Protection, Chase Will Not Allow You to Send Zelle Payments Identified as Originating From Contact Through Social Media* ([www.chase.com/digital/resources/privacy-security/security/social-media-scams](http://www.chase.com/digital/resources/privacy-security/security/social-media-scams)) (accessed Aug. 13, 2025).

<sup>5</sup> Pew Research Center, *From Looking for Love to Swiping the Field: Online Dating in the U.S.* (Feb. 2, 2023) ([www.pewresearch.org/wp-content/uploads/sites/20/2023/01/PI\\_2023.02.02\\_Onilne-Dating\\_FINAL.pdf](http://www.pewresearch.org/wp-content/uploads/sites/20/2023/01/PI_2023.02.02_Onilne-Dating_FINAL.pdf)).

<sup>6</sup> OpenAI, *Disrupting Malicious Uses of Our Models: An Update* (Feb. 2025) ([cdn.openai.com/threat-intelligence-reports/disrupting-malicious-uses-of-our-models-february-2025-update.pdf](https://cdn.openai.com/threat-intelligence-reports/disrupting-malicious-uses-of-our-models-february-2025-update.pdf)).

<sup>7</sup> Government Accountability Office, *Actions Need to Improve Complaint Reporting, Consumer Education, and Federal Coordination to Counter Scams* (GAO-25-107088) (Apr. 2025).

<sup>8</sup> House Committee on Financial Services, Testimony Submitted for the Record of Cyber Policy and Strategy Director Matthew Noyes, Office of Investigations, U.S. Secret Service, *Hearing on Protecting Americans' Savings: Examining the Economics of the Multi-Billion Dollar Romance Confidence Scam Industry*, 118th Cong. (Sep. 18, 2024) (H. Hrg. 118-BA10).

<sup>9</sup> U.S.-China Economic and Security Review Commission, *China's Exploitation of Scam Centers in Southeast Asia* (July 18, 2025) ([www.uscc.gov/sites/default/files/2025-07/Chinas\\_Exploitation\\_of\\_Scam\\_Centers\\_in\\_Southeast\\_Asia.pdf](http://www.uscc.gov/sites/default/files/2025-07/Chinas_Exploitation_of_Scam_Centers_in_Southeast_Asia.pdf)).

rebuild their criminal network.<sup>10</sup> Broken Tooth operates a multi-billion scam network in China's backyard near the Thailand-Myanmar border — reportedly laundering corrupt profits into the failing Chinese real estate sector and spreading CCP propaganda.<sup>11</sup> And as discussed above, scams perpetrated by Chinese criminal networks have devastated U.S. citizens. Last year, an 82-year-old Virginia man named Dennis took his own life due to a scam that resulted in a loss of his life savings.<sup>12</sup>

As the Administration acts to thwart bad actors and their corrosive attacks on our nation, whether in response to fentanyl trafficking or criminal cartel organizations, these scam compounds represent a necessary front.<sup>13</sup> The Government Accountability Office (GAO), for instance, recommended that the Federal Bureau of Investigation lead the development of a government-wide strategy to combat scams that would address the “coordination of federal and business activities.”<sup>14</sup> Industry representatives interviewed for the audit similarly called for what the GAO described as “a multisector approach, to include telecommunications and social media companies, as well as law enforcement to address fraudulently induced payments.”<sup>15</sup> Officials from one of the world's largest financial institutions also expressed support for public and private partnership as part of a whole-of-government response.<sup>16</sup> Similarly, the USCC has argued that improved coordination between the U.S. government and technology companies could be a solution to this problem.<sup>17</sup> With no additional response, however, “criminal groups will likely continue exploiting platforms and services to target Americans with impunity.”<sup>18</sup>

---

<sup>10</sup> *Id.*

<sup>11</sup> *Id.*

<sup>12</sup> *Id.*

<sup>13</sup> U.S. Department of the Treasury: *U.S. and U.K Take Largest Action Ever Targeting Cybercriminal Networks in Southeast Asia* (Oct. 14, 2025); U.S. Department of Justice, *Chairman of Prince Group Indicted for Operating Cambodian Forced Labor Scam Compounds Engaged in Cryptocurrency Fraud Schemes* (Oct. 14, 2025).

<sup>14</sup> House Committee on Financial Services, Testimony Submitted for the Record of Cyber Policy and Strategy Director Matthew Noyes, Office of Investigations, U.S. Secret Service, *Hearing on Protecting Americans' Savings: Examining the Economics of the Multi-Billion Dollar Romance Confidence Scam Industry*, 118th Cong. (Sep. 18, 2024) (H. Hrg. 118-BA10).

<sup>15</sup> *Id.*

<sup>16</sup> *Id.*

<sup>17</sup> U.S.-China Economic and Security Review Commission, *China's Exploitation of Scam Centers in Southeast Asia* (July 18, 2025) ([www.uscc.gov/sites/default/files/2025-07/Chinas\\_Exploitation\\_of\\_Scam\\_Centers\\_in\\_Southeast\\_Asia.pdf](https://www.uscc.gov/sites/default/files/2025-07/Chinas_Exploitation_of_Scam_Centers_in_Southeast_Asia.pdf)).

<sup>18</sup> *Id.*

To aid the Joint Economic Committee in understanding the Treasury's current efforts and engagement with U.S. technology companies to combat overseas scam compounds and the actors that enable these scams, please provide responses to the following information requests:

1. Please identify all U.S. social media, online dating, artificial intelligence, peer-to-peer payment application, and satellite internet service companies with which the Treasury currently engages to disrupt activity from overseas scam compounds and describe the frequency and nature of each engagement.
2. What specific tools or data do U.S. technology companies currently provide to the Treasury as part of these engagements?
3. Please describe any non-confidential coordination between the Treasury, U.S. technology companies, and other federal agencies that led to a federal enforcement action against an overseas scam compound or the foreign actors supporting the compound.
4. Please provide the Treasury's total budget and current full-time equivalent staff dedicated to combating activity from overseas scam compounds.
5. What metrics, if any, does the Treasury use to evaluate the effectiveness of its efforts to combat activity from overseas scam compounds? If the Treasury plans to improve or develop these metrics, please describe how this will be achieved.
6. What dollar amount did the Treasury help save or return to victims of activity from overseas scam compounds in Fiscal Year 2024 and Fiscal Year 2025 to date due to its efforts to combat these scams?
7. Please describe the Treasury's coordination with the following entities to combat activity from overseas scam compounds. For each entity, identify the Treasury offices involved; the scope and frequency of coordination; and any specific initiatives, joint operations, or information-sharing mechanisms:
  - a. Other U.S. federal agencies;
  - b. Foreign government or law enforcement agencies; and
  - c. International government or law enforcement agencies.
8. If the Treasury plans to improve its current coordination activities related to the issues mentioned above, please describe how this will be achieved.
9. What additional tools, if any, would help aid the Treasury in combating criminal scamming networks and the foreign actors supporting these networks?

Please provide your responses as soon as possible but in no event later than January 21, 2026. If you have any questions related to this request, please contact [REDACTED] of the

The Honorable Scott Bessent

December 17, 2025

Page 5

Committee staff at [REDACTED] or [REDACTED]. Please send any official correspondence relating to this request to [REDACTED].

Sincerely,



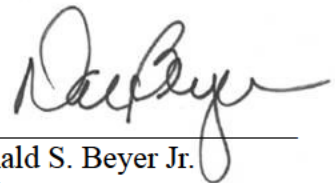
David Schweikert  
Chairman



Eric S. Schmitt  
Vice Chairman



Margaret Wood Hassan  
Ranking Member



Donald S. Beyer Jr.  
Senior House Democrat

## HOUSE OF REPRESENTATIVES

DAVID SCHWEIKERT, ARIZONA, CHAIRMAN  
JODEY C. ARRINGTON, TEXAS  
RON ESTES, KANSAS  
LLOYD K. SMUCKER, PENNSYLVANIA  
NICOLE MALLIOTAKIS, NEW YORK  
VICTORIA SPARTZ, INDIANA

DONALD S. BEYER JR., VIRGINIA  
GWEN MOORE, WISCONSIN  
SEAN CASTEN, ILLINOIS  
DAVE MIN, CALIFORNIA

RON DONADO, EXECUTIVE DIRECTOR

## Congress of the United States

JOINT ECONOMIC COMMITTEE  
(CREATED PURSUANT TO SEC. 5(a) OF PUBLIC LAW 304, 79TH CONGRESS)

Washington, DC 20510-6602

## SENATE

ERIC SCHMITT, MISSOURI, VICE CHAIRMAN  
TOM COTTON, ARKANSAS  
TED BUDD, NORTH CAROLINA  
DAVID MCCORMICK, PENNSYLVANIA  
MARSHA BLACKBURN, TENNESSEE  
ASHLEY MOODY, FLORIDA

MARGARET WOOD HASSAN, NEW HAMPSHIRE,  
RANKING MEMBER  
AMY KLOBUCHAR, MINNESOTA  
MARTIN HEINRICH, NEW MEXICO  
MARK KELLY, ARIZONA

LAURA EPSTEIN, DEMOCRATIC STAFF DIRECTOR

December 17, 2025

The Honorable Marco Rubio  
Secretary of State  
U.S. Department of State  
2201 C Street, NW  
Washington, DC 20520

Dear Secretary Rubio:

We are writing to request information about the ways in which the Department of State (Department) and U.S. technology companies are engaging to disrupt overseas scam networks and protect Americans from fraud and the foreign adversaries that enflame it, as well as the staff and other resources that the Department dedicates to this effort. Last year, overseas scam networks stole an estimated \$10 billion from Americans through sophisticated criminal compounds that are based in Southeast Asia and are often staffed through the forced labor of trafficked workers.<sup>1</sup> These scam compounds often rely on U.S.-based technologies — including social media and online dating platforms, artificial intelligence models, peer-to-peer payment applications, and satellite internet services — to identify, target, and defraud victims. New technology has contributed to the proliferation of these overseas compounds in recent years. Still, “U.S. efforts [to expose and deter this growing threat] remain fragmented and under-resourced,” according to the U.S.-China Economic and Security Review Commission (USCC).<sup>2</sup>

Online scammers overseas routinely use technology or online platforms owned by American companies to defraud victims in the United States. For instance, to begin a scam, criminals frequently initiate contact with potential victims on American-owned social media and online dating platforms. In the first half of 2023, at least half of individuals who reported financial losses from an online romance scam to the Federal Trade Commission (FTC) said that

---

<sup>1</sup> U.S. Department of the Treasury: *U.S. and U.K Take Largest Action Ever Targeting Cybercriminal Networks in Southeast Asia* (Oct. 14, 2025).

<sup>2</sup> U.S.-China Economic and Security Review Commission, *China’s Exploitation of Scam Centers in Southeast Asia* (July 18, 2025) ([www.uscc.gov/sites/default/files/2025-07/Chinas\\_Exploitation\\_of\\_Scam\\_Centers\\_in\\_Southeast\\_Asia.pdf](http://www.uscc.gov/sites/default/files/2025-07/Chinas_Exploitation_of_Scam_Centers_in_Southeast_Asia.pdf)).

the scam began on a social media platform.<sup>3</sup> Similarly, a co-owner of one popular peer-to-peer payment application notes that nearly half of the scams that its consumers report originate on social media.<sup>4</sup> In addition, more than half of online dating users believe that they have encountered a scam.<sup>5</sup> Scammers can also lend credibility to their communications with the use of artificial intelligence models developed and owned by American companies. In a February 2025 report, for example, one leading artificial intelligence company noted that scammers in Cambodia had used its technology to generate personalized English-language messages and sustain conversations with users on social media.<sup>6</sup> Once they gain a victim's trust, overseas scammers then solicit payments through American-owned peer-to-peer payment apps, where transfers are instant and, as the FTC notes, difficult to reverse.<sup>7</sup> Finally, as an official from the U.S. Secret Service testified to Congress, scam compounds in Southeast Asia are increasingly turning to American-owned satellite internet service for the connectivity that often makes these online scams possible.<sup>8</sup>

Moreover, scam compounds in Southeast Asia reportedly operate with the tacit approval of Chinese state actors as part of a symbiotic relationship built on the exploitation of others.<sup>9</sup> As described in the USCC report on these networks, criminal actors like Chinese crime boss Wan Kuok-Koi ("Broken Tooth") have reinvented themselves into pro-CCP businesspeople as they

---

<sup>3</sup> Federal Trade Commission, *Social Media: A Golden Goose for Scammers* ([www.ftc.gov/news-events/data-visualizations/data-spotlight/2023/10/social-media-golden-goose-scammers](http://www.ftc.gov/news-events/data-visualizations/data-spotlight/2023/10/social-media-golden-goose-scammers)) (accessed Aug. 13, 2025).

<sup>4</sup> Chase, *Alert: For Your Protection, Chase Will Not Allow You to Send Zelle Payments Identified as Originating From Contact Through Social Media* ([www.chase.com/digital/resources/privacy-security/security/social-media-scams](http://www.chase.com/digital/resources/privacy-security/security/social-media-scams)) (accessed Aug. 13, 2025).

<sup>5</sup> Pew Research Center, *From Looking for Love to Swiping the Field: Online Dating in the U.S.* (Feb. 2, 2023) ([www.pewresearch.org/wp-content/uploads/sites/20/2023/01/PI\\_2023.02.02\\_Onilne-Dating\\_FINAL.pdf](http://www.pewresearch.org/wp-content/uploads/sites/20/2023/01/PI_2023.02.02_Onilne-Dating_FINAL.pdf)).

<sup>6</sup> OpenAI, *Disrupting Malicious Uses of Our Models: An Update* (Feb. 2025) ([cdn.openai.com/threat-intelligence-reports/disrupting-malicious-uses-of-our-models-february-2025-update.pdf](https://cdn.openai.com/threat-intelligence-reports/disrupting-malicious-uses-of-our-models-february-2025-update.pdf)).

<sup>7</sup> Government Accountability Office, *Actions Need to Improve Complaint Reporting, Consumer Education, and Federal Coordination to Counter Scams* (GAO-25-107088) (Apr. 2025).

<sup>8</sup> House Committee on Financial Services, Testimony Submitted for the Record of Cyber Policy and Strategy Director Matthew Noyes, Office of Investigations, U.S. Secret Service, *Hearing on Protecting Americans' Savings: Examining the Economics of the Multi-Billion Dollar Romance Confidence Scam Industry*, 118th Cong. (Sep. 18, 2024) (H. Hrg. 118-BA10).

<sup>9</sup> U.S.-China Economic and Security Review Commission, *China's Exploitation of Scam Centers in Southeast Asia* (July 18, 2025) ([www.uscc.gov/sites/default/files/2025-07/Chinas\\_Exploitation\\_of\\_Scam\\_Centers\\_in\\_Southeast\\_Asia.pdf](http://www.uscc.gov/sites/default/files/2025-07/Chinas_Exploitation_of_Scam_Centers_in_Southeast_Asia.pdf)).

rebuild their criminal network.<sup>10</sup> Broken Tooth operates a multi-billion scam network in China's backyard near the Thailand-Myanmar border — reportedly laundering corrupt profits into the failing Chinese real estate sector and spreading CCP propaganda.<sup>11</sup> And as discussed above, scams perpetrated by Chinese criminal networks have devastated U.S. citizens. Last year, an 82-year-old Virginia man named Dennis took his own life due to a scam that resulted in a loss of his life savings.<sup>12</sup>

As the Administration acts to thwart bad actors and their corrosive attacks on our nation, whether in response to fentanyl trafficking or criminal cartel organizations, these scam compounds represent a necessary front.<sup>13</sup> The Government Accountability Office (GAO), for instance, recommended that the Federal Bureau of Investigation lead the development of a government-wide strategy to combat scams that would address the “coordination of federal and business activities.”<sup>14</sup> Industry representatives interviewed for the audit similarly called for what the GAO described as “a multisector approach, to include telecommunications and social media companies, as well as law enforcement to address fraudulently induced payments.”<sup>15</sup> Officials from one of the world's largest financial institutions also expressed support for public and private partnership as part of a whole-of-government response.<sup>16</sup> Similarly, the USCC has argued that improved coordination between the U.S. government and technology companies could be a solution to this problem.<sup>17</sup> With no additional response, however, “criminal groups will likely continue exploiting platforms and services to target Americans with impunity.”<sup>18</sup>

---

<sup>10</sup> *Id.*

<sup>11</sup> *Id.*

<sup>12</sup> *Id.*

<sup>13</sup> U.S. Department of the Treasury: *U.S. and U.K Take Largest Action Ever Targeting Cybercriminal Networks in Southeast Asia* (Oct. 14, 2025); U.S. Department of Justice, *Chairman of Prince Group Indicted for Operating Cambodian Forced Labor Scam Compounds Engaged in Cryptocurrency Fraud Schemes* (Oct. 14, 2025).

<sup>14</sup> House Committee on Financial Services, Testimony Submitted for the Record of Cyber Policy and Strategy Director Matthew Noyes, Office of Investigations, U.S. Secret Service, *Hearing on Protecting Americans' Savings: Examining the Economics of the Multi-Billion Dollar Romance Confidence Scam Industry*, 118th Cong. (Sep. 18, 2024) (H. Hrg. 118-BA10).

<sup>15</sup> *Id.*

<sup>16</sup> *Id.*

<sup>17</sup> U.S.-China Economic and Security Review Commission, *China's Exploitation of Scam Centers in Southeast Asia* (July 18, 2025) ([www.uscc.gov/sites/default/files/2025-07/Chinas\\_Exploitation\\_of\\_Scam\\_Centers\\_in\\_Southeast\\_Asia.pdf](https://www.uscc.gov/sites/default/files/2025-07/Chinas_Exploitation_of_Scam_Centers_in_Southeast_Asia.pdf)).

<sup>18</sup> *Id.*



To aid the Joint Economic Committee in understanding the Department's current efforts and engagement with U.S. technology companies to combat overseas scam compounds and the actors that enable these scams, please provide responses to the following information requests:

1. Please identify all U.S. social media, online dating, artificial intelligence, peer-to-peer payment application, and satellite internet service companies with which the Department currently engages to disrupt activity from overseas scam compounds and describe the frequency and nature of each engagement.
2. What specific tools or data do U.S. technology companies currently provide to the Department as part of these engagements?
3. Please describe any non-confidential coordination between the Department, U.S. technology companies, and other federal agencies that led to a federal enforcement action against an overseas scam compound or the foreign actors supporting the compound.
4. Please provide the Department's total budget and current full-time equivalent staff dedicated to combating activity from overseas scam compounds.
5. What metrics, if any, does the Department use to evaluate the effectiveness of its efforts to combat activity from overseas scam compounds? If the Department plans to improve or develop these metrics, please describe how this will be achieved.
6. What dollar amount did the Department help save or return to victims of activity from overseas scam compounds in Fiscal Year 2024 and Fiscal Year 2025 to date due to its efforts to combat these scams?
7. Please describe the Department's coordination with the following entities to combat activity from overseas scam compounds. For each entity, identify the Department offices involved; the scope and frequency of coordination; and any specific initiatives, joint operations, or information-sharing mechanisms:
  - a. Other U.S. federal agencies;
  - b. Foreign government or law enforcement agencies; and
  - c. International government or law enforcement agencies.
8. If the Department plans to improve its current coordination activities related to the issues mentioned above, please describe how this will be achieved.
9. What additional tools, if any, would help aid the Department in combating criminal scamming networks and the foreign actors supporting these networks?

Please provide your responses as soon as possible but in no event later than January 21, 2026. If you have any questions related to this request, please contact [REDACTED] of the

The Honorable Marco Rubio

December 17, 2025

Page 5

Committee staff at [REDACTED] or [REDACTED]. Please send any official correspondence relating to this request to [REDACTED].

Sincerely,



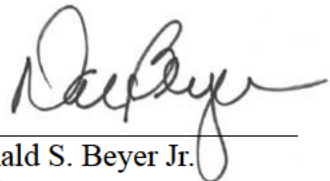
David Schweikert  
Chairman



Eric S. Schmitt  
Vice Chairman



Margaret Wood Hassan  
Ranking Member



Donald S. Beyer Jr.  
Senior House Democrat

## HOUSE OF REPRESENTATIVES

DAVID SCHWEIKERT, ARIZONA, CHAIRMAN  
JODEY C. ARRINGTON, TEXAS  
RON ESTES, KANSAS  
LLOYD K. SMUCKER, PENNSYLVANIA  
NICOLE MALLIOTAKIS, NEW YORK  
VICTORIA SPARTZ, INDIANA

DONALD S. BEYER JR., VIRGINIA  
GWEN MOORE, WISCONSIN  
SEAN CASTEN, ILLINOIS  
DAVE MIN, CALIFORNIA

RON DONADO, EXECUTIVE DIRECTOR

## Congress of the United States

JOINT ECONOMIC COMMITTEE  
(CREATED PURSUANT TO SEC. 5(a) OF PUBLIC LAW 304, 79TH CONGRESS)

Washington, DC 20510-6602

## SENATE

ERIC SCHMITT, MISSOURI, VICE CHAIRMAN  
TOM COTTON, ARKANSAS  
TED BUDD, NORTH CAROLINA  
DAVID MCCORMICK, PENNSYLVANIA  
MARSHA BLACKBURN, TENNESSEE  
ASHLEY MOODY, FLORIDA

MARGARET WOOD HASSAN, NEW HAMPSHIRE,  
RANKING MEMBER  
AMY KLOBUCHAR, MINNESOTA  
MARTIN HEINRICH, NEW MEXICO  
MARK KELLY, ARIZONA

LAURA EPSTEIN, DEMOCRATIC STAFF DIRECTOR

December 17, 2025

The Honorable Andrew N. Ferguson  
Chairman  
Federal Trade Commission  
600 Pennsylvania Avenue, NW  
Washington, DC 20580

Dear Chairman Ferguson:

We are writing to request information about the ways in which the Federal Trade Commission (FTC) and U.S. technology companies are engaging to disrupt overseas scam networks and protect Americans from fraud and the foreign adversaries that enflame it, as well as the staff and other resources that the FTC dedicates to this effort. Last year, overseas scam networks stole an estimated \$10 billion from Americans through sophisticated criminal compounds that are based in Southeast Asia and are often staffed through the forced labor of trafficked workers.<sup>1</sup> These scam compounds often rely on U.S.-based technologies — including social media and online dating platforms, artificial intelligence models, peer-to-peer payment applications, and satellite internet services — to identify, target, and defraud victims. New technology has contributed to the proliferation of these overseas compounds in recent years. Still, “U.S. efforts [to expose and deter this growing threat] remain fragmented and under-resourced,” according to the U.S.-China Economic and Security Review Commission (USCC).<sup>2</sup>

Online scammers overseas routinely use technology or online platforms owned by American companies to defraud victims in the United States. For instance, to begin a scam, criminals frequently initiate contact with potential victims on American-owned social media and online dating platforms. In the first half of 2023, at least half of individuals who reported financial losses from an online romance scam to the FTC said that the scam began on a social

---

<sup>1</sup> U.S. Department of the Treasury: *U.S. and U.K Take Largest Action Ever Targeting Cybercriminal Networks in Southeast Asia* (Oct. 14, 2025).

<sup>2</sup> U.S.-China Economic and Security Review Commission, *China’s Exploitation of Scam Centers in Southeast Asia* (July 18, 2025) ([www.uscc.gov/sites/default/files/2025-07/Chinas\\_Exploitation\\_of\\_Scam\\_Centers\\_in\\_Southeast\\_Asia.pdf](http://www.uscc.gov/sites/default/files/2025-07/Chinas_Exploitation_of_Scam_Centers_in_Southeast_Asia.pdf)).

media platform.<sup>3</sup> Similarly, a co-owner of one popular peer-to-peer payment application notes that nearly half of the scams that its consumers report originate on social media.<sup>4</sup> In addition, more than half of online dating users believe that they have encountered a scam.<sup>5</sup> Scammers can also lend credibility to their communications with the use of artificial intelligence models developed and owned by American companies. In a February 2025 report, for example, one leading artificial intelligence company noted that scammers in Cambodia had used its technology to generate personalized English-language messages and sustain conversations with users on social media.<sup>6</sup> Once they gain a victim's trust, overseas scammers then solicit payments through American-owned peer-to-peer payment apps, where transfers are instant and, as the FTC notes, difficult to reverse.<sup>7</sup> Finally, as an official from the U.S. Secret Service testified to Congress, scam compounds in Southeast Asia are increasingly turning to American-owned satellite internet service for the connectivity that often makes these online scams possible.<sup>8</sup>

Moreover, scam compounds in Southeast Asia reportedly operate with the tacit approval of Chinese state actors as part of a symbiotic relationship built on the exploitation of others.<sup>9</sup> As described in the USCC report on these networks, criminal actors like Chinese crime boss Wan Kuok-Koi ("Broken Tooth") have reinvented themselves into pro-CCP businesspeople as they

---

<sup>3</sup> Federal Trade Commission, *Social Media: A Golden Goose for Scammers* ([www.ftc.gov/news-events/data-visualizations/data-spotlight/2023/10/social-media-golden-goose-scammers](http://www.ftc.gov/news-events/data-visualizations/data-spotlight/2023/10/social-media-golden-goose-scammers)) (accessed Aug. 13, 2025).

<sup>4</sup> Chase, *Alert: For Your Protection, Chase Will Not Allow You to Send Zelle Payments Identified as Originating From Contact Through Social Media* ([www.chase.com/digital/resources/privacy-security/security/social-media-scams](http://www.chase.com/digital/resources/privacy-security/security/social-media-scams)) (accessed Aug. 13, 2025).

<sup>5</sup> Pew Research Center, *From Looking for Love to Swiping the Field: Online Dating in the U.S.* (Feb. 2, 2023) ([www.pewresearch.org/wp-content/uploads/sites/20/2023/01/PI\\_2023.02.02\\_Onilne-Dating\\_FINAL.pdf](http://www.pewresearch.org/wp-content/uploads/sites/20/2023/01/PI_2023.02.02_Onilne-Dating_FINAL.pdf)).

<sup>6</sup> OpenAI, *Disrupting Malicious Uses of Our Models: An Update* (Feb. 2025) ([cdn.openai.com/threat-intelligence-reports/disrupting-malicious-uses-of-our-models-february-2025-update.pdf](https://cdn.openai.com/threat-intelligence-reports/disrupting-malicious-uses-of-our-models-february-2025-update.pdf)).

<sup>7</sup> Government Accountability Office, *Actions Need to Improve Complaint Reporting, Consumer Education, and Federal Coordination to Counter Scams* (GAO-25-107088) (Apr. 2025).

<sup>8</sup> House Committee on Financial Services, Testimony Submitted for the Record of Cyber Policy and Strategy Director Matthew Noyes, Office of Investigations, U.S. Secret Service, *Hearing on Protecting Americans' Savings: Examining the Economics of the Multi-Billion Dollar Romance Confidence Scam Industry*, 118th Cong. (Sep. 18, 2024) (H. Hrg. 118-BA10).

<sup>9</sup> U.S.-China Economic and Security Review Commission, *China's Exploitation of Scam Centers in Southeast Asia* (July 18, 2025) ([www.uscc.gov/sites/default/files/2025-07/Chinas\\_Exploitation\\_of\\_Scam\\_Centers\\_in\\_Southeast\\_Asia.pdf](http://www.uscc.gov/sites/default/files/2025-07/Chinas_Exploitation_of_Scam_Centers_in_Southeast_Asia.pdf)).

rebuild their criminal network.<sup>10</sup> Broken Tooth operates a multi-billion scam network in China's backyard near the Thailand-Myanmar border — reportedly laundering corrupt profits into the failing Chinese real estate sector and spreading CCP propaganda.<sup>11</sup> And as discussed above, scams perpetrated by Chinese criminal networks have devastated U.S. citizens. Last year, an 82-year-old Virginia man named Dennis took his own life due to a scam that resulted in a loss of his life savings.<sup>12</sup>

As the Administration acts to thwart bad actors and their corrosive attacks on our nation, whether in response to fentanyl trafficking or criminal cartel organizations, these scam compounds represent a necessary front.<sup>13</sup> The Government Accountability Office (GAO), for instance, recommended that the Federal Bureau of Investigation lead the development of a government-wide strategy to combat scams that would address the “coordination of federal and business activities.”<sup>14</sup> Industry representatives interviewed for the audit similarly called for what the GAO described as “a multisector approach, to include telecommunications and social media companies, as well as law enforcement to address fraudulently induced payments.”<sup>15</sup> Officials from one of the world's largest financial institutions also expressed support for public and private partnership as part of a whole-of-government response.<sup>16</sup> Similarly, the USCC has argued that improved coordination between the U.S. government and technology companies could be a solution to this problem.<sup>17</sup> With no additional response, however, “criminal groups will likely continue exploiting platforms and services to target Americans with impunity.”<sup>18</sup>

---

<sup>10</sup> *Id.*

<sup>11</sup> *Id.*

<sup>12</sup> *Id.*

<sup>13</sup> U.S. Department of the Treasury: *U.S. and U.K Take Largest Action Ever Targeting Cybercriminal Networks in Southeast Asia* (Oct. 14, 2025); U.S. Department of Justice, *Chairman of Prince Group Indicted for Operating Cambodian Forced Labor Scam Compounds Engaged in Cryptocurrency Fraud Schemes* (Oct. 14, 2025).

<sup>14</sup> House Committee on Financial Services, Testimony Submitted for the Record of Cyber Policy and Strategy Director Matthew Noyes, Office of Investigations, U.S. Secret Service, *Hearing on Protecting Americans' Savings: Examining the Economics of the Multi-Billion Dollar Romance Confidence Scam Industry*, 118th Cong. (Sep. 18, 2024) (H. Hrg. 118-BA10).

<sup>15</sup> *Id.*

<sup>16</sup> *Id.*

<sup>17</sup> U.S.-China Economic and Security Review Commission, *China's Exploitation of Scam Centers in Southeast Asia* (July 18, 2025) ([www.uscc.gov/sites/default/files/2025-07/Chinas\\_Exploitation\\_of\\_Scam\\_Centers\\_in\\_Southeast\\_Asia.pdf](https://www.uscc.gov/sites/default/files/2025-07/Chinas_Exploitation_of_Scam_Centers_in_Southeast_Asia.pdf)).

<sup>18</sup> *Id.*

To aid the Joint Economic Committee in understanding the FTC's current efforts and engagement with U.S. technology companies to combat overseas scam compounds and the actors that enable these scams, please provide responses to the following information requests:

1. Please identify all U.S. social media, online dating, artificial intelligence, peer-to-peer payment application, and satellite internet service companies with which the FTC currently engages to disrupt activity from overseas scam compounds and describe the frequency and nature of each engagement.
2. What specific tools or data do U.S. technology companies currently provide to the FTC as part of these engagements?
3. Please describe any non-confidential coordination between the FTC, U.S. technology companies, and other federal agencies that led to a federal enforcement action against an overseas scam compound or the foreign actors supporting the compound.
4. Please provide the FTC's total budget and current full-time equivalent staff dedicated to combating activity from overseas scam compounds.
5. What metrics, if any, does the FTC use to evaluate the effectiveness of its efforts to combat activity from overseas scam compounds? If the FTC plans to improve or develop these metrics, please describe how this will be achieved.
6. What dollar amount did the FTC help save or return to victims of activity from overseas scam compounds in Fiscal Year 2024 and Fiscal Year 2025 to date due to its efforts to combat these scams?
7. Please describe the FTC's coordination with the following entities to combat activity from overseas scam compounds. For each entity, identify the FTC offices involved; the scope and frequency of coordination; and any specific initiatives, joint operations, or information-sharing mechanisms:
  - a. Other U.S. federal agencies;
  - b. Foreign government or law enforcement agencies; and
  - c. International government or law enforcement agencies.
8. If the FTC plans to improve its current coordination activities related to the issues mentioned above, please describe how this will be achieved.
9. What additional tools, if any, would help aid the FTC in combating criminal scamming networks and the foreign actors supporting these networks?

Please provide your responses as soon as possible but in no event later than January 21, 2026. If you have any questions related to this request, please contact [REDACTED] of the Committee staff at [REDACTED] or [REDACTED]. Please send any official correspondence relating to this request to [REDACTED].

Sincerely,

A handwritten signature in blue ink, appearing to read "David Schweikert", written in a cursive style.

---

David Schweikert  
Chairman

A handwritten signature in blue ink, appearing to read "Eric S. Schmitt", written in a cursive style.

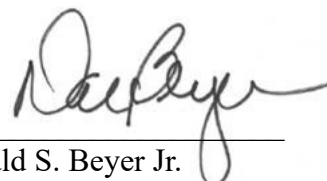
---

Eric S. Schmitt  
Vice Chairman

A handwritten signature in blue ink, appearing to read "Margaret Wood Hassan", written in a cursive style.

---

Margaret Wood Hassan  
Ranking Member

A handwritten signature in blue ink, appearing to read "Donald S. Beyer Jr.", written in a cursive style.

---

Donald S. Beyer Jr.  
Senior House Democrat

## HOUSE OF REPRESENTATIVES

DAVID SCHWEIKERT, ARIZONA, CHAIRMAN  
JODEY C. ARRINGTON, TEXAS  
RON ESTES, KANSAS  
LLOYD K. SMUCKER, PENNSYLVANIA  
NICOLE MALLIOTAKIS, NEW YORK  
VICTORIA SPARTZ, INDIANA

DONALD S. BEYER JR., VIRGINIA  
GWEN MOORE, WISCONSIN  
SEAN CASTEN, ILLINOIS  
DAVE MIN, CALIFORNIA

RON DONADO, EXECUTIVE DIRECTOR

## Congress of the United States

JOINT ECONOMIC COMMITTEE  
(CREATED PURSUANT TO SEC. 5(a) OF PUBLIC LAW 304, 79TH CONGRESS)

Washington, DC 20510-6602

## SENATE

ERIC SCHMITT, MISSOURI, VICE CHAIRMAN  
TOM COTTON, ARKANSAS  
TED BUDD, NORTH CAROLINA  
DAVID MCCORMICK, PENNSYLVANIA  
MARSHA BLACKBURN, TENNESSEE  
ASHLEY MOODY, FLORIDA

MARGARET WOOD HASSAN, NEW HAMPSHIRE,  
RANKING MEMBER  
AMY KLOBUCHAR, MINNESOTA  
MARTIN HEINRICH, NEW MEXICO  
MARK KELLY, ARIZONA

LAURA EPSTEIN, DEMOCRATIC STAFF DIRECTOR

December 17, 2025

The Honorable Pamela Bondi  
Attorney General  
U.S. Department of Justice  
950 Pennsylvania Ave NW  
Washington, DC 20530

Dear Attorney General Bondi:

We are writing to request information about the ways in which the Department of Justice (DOJ) and U.S. technology companies are engaging to disrupt overseas scam networks and protect Americans from fraud and the foreign adversaries that enflame it, as well as the staff and other resources that the DOJ dedicates to this effort. Last year, overseas scam networks stole an estimated \$10 billion from Americans through sophisticated criminal compounds that are based in Southeast Asia and are often staffed through the forced labor of trafficked workers.<sup>1</sup> These scam compounds often rely on U.S.-based technologies — including social media and online dating platforms, artificial intelligence models, peer-to-peer payment applications, and satellite internet services — to identify, target, and defraud victims. New technology has contributed to the proliferation of these overseas compounds in recent years. Still, “U.S. efforts [to expose and deter this growing threat] remain fragmented and under-resourced,” according to the U.S.-China Economic and Security Review Commission (USCC).<sup>2</sup>

Online scammers overseas routinely use technology or online platforms owned by American companies to defraud victims in the United States. For instance, to begin a scam, criminals frequently initiate contact with potential victims on American-owned social media and online dating platforms. In the first half of 2023, at least half of individuals who reported financial losses from an online romance scam to the Federal Trade Commission (FTC) said that

---

<sup>1</sup> U.S. Department of the Treasury: *U.S. and U.K Take Largest Action Ever Targeting Cybercriminal Networks in Southeast Asia* (Oct. 14, 2025).

<sup>2</sup> U.S.-China Economic and Security Review Commission, *China’s Exploitation of Scam Centers in Southeast Asia* (July 18, 2025) ([www.uscc.gov/sites/default/files/2025-07/Chinas\\_Exploitation\\_of\\_Scam\\_Centers\\_in\\_Southeast\\_Asia.pdf](http://www.uscc.gov/sites/default/files/2025-07/Chinas_Exploitation_of_Scam_Centers_in_Southeast_Asia.pdf)).



the scam began on a social media platform.<sup>3</sup> Similarly, a co-owner of one popular peer-to-peer payment application notes that nearly half of the scams that its consumers report originate on social media.<sup>4</sup> In addition, more than half of online dating users believe that they have encountered a scam.<sup>5</sup> Scammers can also lend credibility to their communications with the use of artificial intelligence models developed and owned by American companies. In a February 2025 report, for example, one leading artificial intelligence company noted that scammers in Cambodia had used its technology to generate personalized English-language messages and sustain conversations with users on social media.<sup>6</sup> Once they gain a victim's trust, overseas scammers then solicit payments through American-owned peer-to-peer payment apps, where transfers are instant and, as the FTC notes, difficult to reverse.<sup>7</sup> Finally, as an official from the U.S. Secret Service testified to Congress, scam compounds in Southeast Asia are increasingly turning to American-owned satellite internet service for the connectivity that often makes these online scams possible.<sup>8</sup>

Moreover, scam compounds in Southeast Asia reportedly operate with the tacit approval of Chinese state actors as part of a symbiotic relationship built on the exploitation of others.<sup>9</sup> As described in the USCC report on these networks, criminal actors like Chinese crime boss Wan Kuok-Koi ("Broken Tooth") have reinvented themselves into pro-CCP businesspeople as they

---

<sup>3</sup> Federal Trade Commission, *Social Media: A Golden Goose for Scammers* ([www.ftc.gov/news-events/data-visualizations/data-spotlight/2023/10/social-media-golden-goose-scammers](http://www.ftc.gov/news-events/data-visualizations/data-spotlight/2023/10/social-media-golden-goose-scammers)) (accessed Aug. 13, 2025).

<sup>4</sup> Chase, *Alert: For Your Protection, Chase Will Not Allow You to Send Zelle Payments Identified as Originating From Contact Through Social Media* ([www.chase.com/digital/resources/privacy-security/security/social-media-scams](http://www.chase.com/digital/resources/privacy-security/security/social-media-scams)) (accessed Aug. 13, 2025).

<sup>5</sup> Pew Research Center, *From Looking for Love to Swiping the Field: Online Dating in the U.S.* (Feb. 2, 2023) ([www.pewresearch.org/wp-content/uploads/sites/20/2023/01/PI\\_2023.02.02\\_Onilne-Dating\\_FINAL.pdf](http://www.pewresearch.org/wp-content/uploads/sites/20/2023/01/PI_2023.02.02_Onilne-Dating_FINAL.pdf)).

<sup>6</sup> OpenAI, *Disrupting Malicious Uses of Our Models: An Update* (Feb. 2025) ([cdn.openai.com/threat-intelligence-reports/disrupting-malicious-uses-of-our-models-february-2025-update.pdf](https://cdn.openai.com/threat-intelligence-reports/disrupting-malicious-uses-of-our-models-february-2025-update.pdf)).

<sup>7</sup> Government Accountability Office, *Actions Need to Improve Complaint Reporting, Consumer Education, and Federal Coordination to Counter Scams* (GAO-25-107088) (Apr. 2025).

<sup>8</sup> House Committee on Financial Services, *Testimony Submitted for the Record of Cyber Policy and Strategy Director Matthew Noyes, Office of Investigations, U.S. Secret Service, Hearing on Protecting Americans' Savings: Examining the Economics of the Multi-Billion Dollar Romance Confidence Scam Industry*, 118th Cong. (Sep. 18, 2024) (H. Hrg. 118-BA10).

<sup>9</sup> U.S.-China Economic and Security Review Commission, *China's Exploitation of Scam Centers in Southeast Asia* (July 18, 2025) ([www.uscc.gov/sites/default/files/2025-07/Chinas\\_Exploitation\\_of\\_Scam\\_Centers\\_in\\_Southeast\\_Asia.pdf](http://www.uscc.gov/sites/default/files/2025-07/Chinas_Exploitation_of_Scam_Centers_in_Southeast_Asia.pdf)).

rebuild their criminal network.<sup>10</sup> Broken Tooth operates a multi-billion scam network in China's backyard near the Thailand-Myanmar border — reportedly laundering corrupt profits into the failing Chinese real estate sector and spreading CCP propaganda.<sup>11</sup> And as discussed above, scams perpetrated by Chinese criminal networks have devastated U.S. citizens. Last year, an 82-year-old Virginia man named Dennis took his own life due to a scam that resulted in a loss of his life savings.<sup>12</sup>

As the Administration acts to thwart bad actors and their corrosive attacks on our nation, whether in response to fentanyl trafficking or criminal cartel organizations, these scam compounds represent a necessary front.<sup>13</sup> The Government Accountability Office (GAO), for instance, recommended that the Federal Bureau of Investigation lead the development of a government-wide strategy to combat scams that would address the “coordination of federal and business activities.”<sup>14</sup> Industry representatives interviewed for the audit similarly called for what the GAO described as “a multisector approach, to include telecommunications and social media companies, as well as law enforcement to address fraudulently induced payments.”<sup>15</sup> Officials from one of the world's largest financial institutions also expressed support for public and private partnership as part of a whole-of-government response.<sup>16</sup> Similarly, the USCC has argued that improved coordination between the U.S. government and technology companies could be a solution to this problem.<sup>17</sup> With no additional response, however, “criminal groups will likely continue exploiting platforms and services to target Americans with impunity.”<sup>18</sup>

---

<sup>10</sup> *Id.*

<sup>11</sup> *Id.*

<sup>12</sup> *Id.*

<sup>13</sup> U.S. Department of the Treasury: *U.S. and U.K Take Largest Action Ever Targeting Cybercriminal Networks in Southeast Asia* (Oct. 14, 2025); U.S. Department of Justice, *Chairman of Prince Group Indicted for Operating Cambodian Forced Labor Scam Compounds Engaged in Cryptocurrency Fraud Schemes* (Oct. 14, 2025).

<sup>14</sup> House Committee on Financial Services, Testimony Submitted for the Record of Cyber Policy and Strategy Director Matthew Noyes, Office of Investigations, U.S. Secret Service, *Hearing on Protecting Americans' Savings: Examining the Economics of the Multi-Billion Dollar Romance Confidence Scam Industry*, 118th Cong. (Sep. 18, 2024) (H. Hrg. 118-BA10).

<sup>15</sup> *Id.*

<sup>16</sup> *Id.*

<sup>17</sup> U.S.-China Economic and Security Review Commission, *China's Exploitation of Scam Centers in Southeast Asia* (July 18, 2025) ([www.uscc.gov/sites/default/files/2025-07/Chinas\\_Exploitation\\_of\\_Scam\\_Centers\\_in\\_Southeast\\_Asia.pdf](https://www.uscc.gov/sites/default/files/2025-07/Chinas_Exploitation_of_Scam_Centers_in_Southeast_Asia.pdf)).

<sup>18</sup> *Id.*

To aid the Joint Economic Committee in understanding the DOJ's current efforts and engagement with U.S. technology companies to combat overseas scam compounds and the actors that enable these scams, please provide responses to the following information requests:

1. Please identify all U.S. social media, online dating, artificial intelligence, peer-to-peer payment application, and satellite internet service companies with which the DOJ currently engages to disrupt activity from overseas scam compounds and describe the frequency and nature of each engagement.
2. What specific tools or data do U.S. technology companies currently provide to the DOJ as part of these engagements?
3. Please describe any non-confidential coordination between the DOJ, U.S. technology companies, and other federal agencies that led to a federal enforcement action against an overseas scam compound or the foreign actors supporting the compound.
4. Please provide the DOJ's total budget and current full-time equivalent staff dedicated to combating activity from overseas scam compounds.
5. What metrics, if any, does the DOJ use to evaluate the effectiveness of its efforts to combat activity from overseas scam compounds? If the DOJ plans to improve or develop these metrics, please describe how this will be achieved.
6. What dollar amount did the DOJ help save or return to victims of activity from overseas scam compounds in Fiscal Year 2024 and Fiscal Year 2025 to date due to its efforts to combat these scams?
7. Please describe the DOJ's coordination with the following entities to combat activity from overseas scam compounds. For each entity, identify the DOJ offices involved; the scope and frequency of coordination; and any specific initiatives, joint operations, or information-sharing mechanisms:
  - a. Other U.S. federal agencies;
  - b. Foreign government or law enforcement agencies; and
  - c. International government or law enforcement agencies.
8. If the DOJ plans to improve its current coordination activities related to the issues mentioned above, please describe how this will be achieved.
9. What additional tools, if any, would help aid the DOJ in combating criminal scamming networks and the foreign actors supporting these networks?

Please provide your responses as soon as possible but in no event later than January 21, 2026. If you have any questions related to this request, please contact [REDACTED] of the Committee staff at [REDACTED] or [REDACTED]. Please send any official correspondence relating to this request to [REDACTED].

Sincerely,



---

David Schweikert  
Chairman



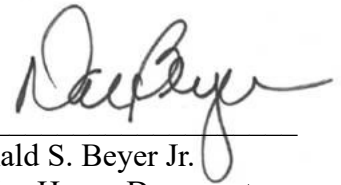
---

Eric S. Schmitt  
Vice Chairman



---

Margaret Wood Hassan  
Ranking Member



---

Donald S. Beyer Jr.  
Senior House Democrat

## HOUSE OF REPRESENTATIVES

DAVID SCHWEIKERT, ARIZONA, CHAIRMAN  
JODEY C. ARRINGTON, TEXAS  
RON ESTES, KANSAS  
LLOYD K. SMUCKER, PENNSYLVANIA  
NICOLE MALLIOTAKIS, NEW YORK  
VICTORIA SPARTZ, INDIANA

DONALD S. BEYER JR., VIRGINIA  
GWEN MOORE, WISCONSIN  
SEAN CASTEN, ILLINOIS  
DAVE MIN, CALIFORNIA

RON DONADO, EXECUTIVE DIRECTOR

## Congress of the United States

JOINT ECONOMIC COMMITTEE  
(CREATED PURSUANT TO SEC. 5(a) OF PUBLIC LAW 304, 79TH CONGRESS)

Washington, DC 20510-6602

## SENATE

ERIC SCHMITT, MISSOURI, VICE CHAIRMAN  
TOM COTTON, ARKANSAS  
TED BUDD, NORTH CAROLINA  
DAVID MCCORMICK, PENNSYLVANIA  
MARSHA BLACKBURN, TENNESSEE  
ASHLEY MOODY, FLORIDA

MARGARET WOOD HASSAN, NEW HAMPSHIRE,  
RANKING MEMBER  
AMY KLOBUCHAR, MINNESOTA  
MARTIN HEINRICH, NEW MEXICO  
MARK KELLY, ARIZONA

LAURA EPSTEIN, DEMOCRATIC STAFF DIRECTOR

December 17, 2025

The Honorable Kristi Noem  
Secretary of Homeland Security  
U.S. Department of Homeland Security  
2707 Martin Luther King Jr. Avenue SE  
Washington, DC 20528

Dear Secretary Noem:

We are writing to request information about the ways in which the Department of Homeland Security (DHS) and U.S. technology companies are engaging to disrupt overseas scam networks and protect Americans from fraud and the foreign adversaries that enflame it, as well as the staff and other resources that the DHS dedicates to this effort. Last year, overseas scam networks stole an estimated \$10 billion from Americans through sophisticated criminal compounds that are based in Southeast Asia and are often staffed through the forced labor of trafficked workers.<sup>1</sup> These scam compounds often rely on U.S.-based technologies — including social media and online dating platforms, artificial intelligence models, peer-to-peer payment applications, and satellite internet services — to identify, target, and defraud victims. New technology has contributed to the proliferation of these overseas compounds in recent years. Still, “U.S. efforts [to expose and deter this growing threat] remain fragmented and under-resourced,” according to the U.S.-China Economic and Security Review Commission (USCC).<sup>2</sup>

Online scammers overseas routinely use technology or online platforms owned by American companies to defraud victims in the United States. For instance, to begin a scam, criminals frequently initiate contact with potential victims on American-owned social media and online dating platforms. In the first half of 2023, at least half of individuals who reported financial losses from an online romance scam to the Federal Trade Commission (FTC) said that

---

<sup>1</sup> U.S. Department of the Treasury: *U.S. and U.K Take Largest Action Ever Targeting Cybercriminal Networks in Southeast Asia* (Oct. 14, 2025).

<sup>2</sup> U.S.-China Economic and Security Review Commission, *China’s Exploitation of Scam Centers in Southeast Asia* (July 18, 2025) ([www.uscc.gov/sites/default/files/2025-07/Chinas\\_Exploitation\\_of\\_Scam\\_Centers\\_in\\_Southeast\\_Asia.pdf](http://www.uscc.gov/sites/default/files/2025-07/Chinas_Exploitation_of_Scam_Centers_in_Southeast_Asia.pdf)).

the scam began on a social media platform.<sup>3</sup> Similarly, a co-owner of one popular peer-to-peer payment application notes that nearly half of the scams that its consumers report originate on social media.<sup>4</sup> In addition, more than half of online dating users believe that they have encountered a scam.<sup>5</sup> Scammers can also lend credibility to their communications with the use of artificial intelligence models developed and owned by American companies. In a February 2025 report, for example, one leading artificial intelligence company noted that scammers in Cambodia had used its technology to generate personalized English-language messages and sustain conversations with users on social media.<sup>6</sup> Once they gain a victim's trust, overseas scammers then solicit payments through American-owned peer-to-peer payment apps, where transfers are instant and, as the FTC notes, difficult to reverse.<sup>7</sup> Finally, as an official from the U.S. Secret Service testified to Congress, scam compounds in Southeast Asia are increasingly turning to American-owned satellite internet service for the connectivity that often makes these online scams possible.<sup>8</sup>

Moreover, scam compounds in Southeast Asia reportedly operate with the tacit approval of Chinese state actors as part of a symbiotic relationship built on the exploitation of others.<sup>9</sup> As described in the USCC report on these networks, criminal actors like Chinese crime boss Wan Kuok-Koi ("Broken Tooth") have reinvented themselves into pro-CCP businesspeople as they

---

<sup>3</sup> Federal Trade Commission, *Social Media: A Golden Goose for Scammers* ([www.ftc.gov/news-events/data-visualizations/data-spotlight/2023/10/social-media-golden-goose-scammers](http://www.ftc.gov/news-events/data-visualizations/data-spotlight/2023/10/social-media-golden-goose-scammers)) (accessed Aug. 13, 2025).

<sup>4</sup> Chase, *Alert: For Your Protection, Chase Will Not Allow You to Send Zelle Payments Identified as Originating From Contact Through Social Media* ([www.chase.com/digital/resources/privacy-security/security/social-media-scams](http://www.chase.com/digital/resources/privacy-security/security/social-media-scams)) (accessed Aug. 13, 2025).

<sup>5</sup> Pew Research Center, *From Looking for Love to Swiping the Field: Online Dating in the U.S.* (Feb. 2, 2023) ([www.pewresearch.org/wp-content/uploads/sites/20/2023/01/PI\\_2023.02.02\\_Onilne-Dating\\_FINAL.pdf](http://www.pewresearch.org/wp-content/uploads/sites/20/2023/01/PI_2023.02.02_Onilne-Dating_FINAL.pdf)).

<sup>6</sup> OpenAI, *Disrupting Malicious Uses of Our Models: An Update* (Feb. 2025) ([cdn.openai.com/threat-intelligence-reports/disrupting-malicious-uses-of-our-models-february-2025-update.pdf](https://cdn.openai.com/threat-intelligence-reports/disrupting-malicious-uses-of-our-models-february-2025-update.pdf)).

<sup>7</sup> Government Accountability Office, *Actions Need to Improve Complaint Reporting, Consumer Education, and Federal Coordination to Counter Scams* (GAO-25-107088) (Apr. 2025).

<sup>8</sup> House Committee on Financial Services, *Testimony Submitted for the Record of Cyber Policy and Strategy Director Matthew Noyes, Office of Investigations, U.S. Secret Service, Hearing on Protecting Americans' Savings: Examining the Economics of the Multi-Billion Dollar Romance Confidence Scam Industry*, 118th Cong. (Sep. 18, 2024) (H. Hrg. 118-BA10).

<sup>9</sup> U.S.-China Economic and Security Review Commission, *China's Exploitation of Scam Centers in Southeast Asia* (July 18, 2025) ([www.uscc.gov/sites/default/files/2025-07/Chinas\\_Exploitation\\_of\\_Scam\\_Centers\\_in\\_Southeast\\_Asia.pdf](http://www.uscc.gov/sites/default/files/2025-07/Chinas_Exploitation_of_Scam_Centers_in_Southeast_Asia.pdf)).

rebuild their criminal network.<sup>10</sup> Broken Tooth operates a multi-billion scam network in China's backyard near the Thailand-Myanmar border — reportedly laundering corrupt profits into the failing Chinese real estate sector and spreading CCP propaganda.<sup>11</sup> And as discussed above, scams perpetrated by Chinese criminal networks have devastated U.S. citizens. Last year, an 82-year-old Virginia man named Dennis took his own life due to a scam that resulted in a loss of his life savings.<sup>12</sup>

As the Administration acts to thwart bad actors and their corrosive attacks on our nation, whether in response to fentanyl trafficking or criminal cartel organizations, these scam compounds represent a necessary front.<sup>13</sup> The Government Accountability Office (GAO), for instance, recommended that the Federal Bureau of Investigation lead the development of a government-wide strategy to combat scams that would address the “coordination of federal and business activities.”<sup>14</sup> Industry representatives interviewed for the audit similarly called for what the GAO described as “a multisector approach, to include telecommunications and social media companies, as well as law enforcement to address fraudulently induced payments.”<sup>15</sup> Officials from one of the world's largest financial institutions also expressed support for public and private partnership as part of a whole-of-government response.<sup>16</sup> Similarly, the USCC has argued that improved coordination between the U.S. government and technology companies could be a solution to this problem.<sup>17</sup> With no additional response, however, “criminal groups will likely continue exploiting platforms and services to target Americans with impunity.”<sup>18</sup>

---

<sup>10</sup> *Id.*

<sup>11</sup> *Id.*

<sup>12</sup> *Id.*

<sup>13</sup> U.S. Department of the Treasury: *U.S. and U.K Take Largest Action Ever Targeting Cybercriminal Networks in Southeast Asia* (Oct. 14, 2025); U.S. Department of Justice, *Chairman of Prince Group Indicted for Operating Cambodian Forced Labor Scam Compounds Engaged in Cryptocurrency Fraud Schemes* (Oct. 14, 2025).

<sup>14</sup> House Committee on Financial Services, Testimony Submitted for the Record of Cyber Policy and Strategy Director Matthew Noyes, Office of Investigations, U.S. Secret Service, *Hearing on Protecting Americans' Savings: Examining the Economics of the Multi-Billion Dollar Romance Confidence Scam Industry*, 118th Cong. (Sep. 18, 2024) (H. Hrg. 118-BA10).

<sup>15</sup> *Id.*

<sup>16</sup> *Id.*

<sup>17</sup> U.S.-China Economic and Security Review Commission, *China's Exploitation of Scam Centers in Southeast Asia* (July 18, 2025) ([www.uscc.gov/sites/default/files/2025-07/Chinas\\_Exploitation\\_of\\_Scam\\_Centers\\_in\\_Southeast\\_Asia.pdf](https://www.uscc.gov/sites/default/files/2025-07/Chinas_Exploitation_of_Scam_Centers_in_Southeast_Asia.pdf)).

<sup>18</sup> *Id.*



To aid the Joint Economic Committee in understanding the DHS's current efforts and engagement with U.S. technology companies to combat overseas scam compounds and the actors that enable these scams, please provide responses to the following information requests:

1. Please identify all U.S. social media, online dating, artificial intelligence, peer-to-peer payment application, and satellite internet service companies with which the DHS currently engages to disrupt activity from overseas scam compounds and describe the frequency and nature of each engagement.
2. What specific tools or data do U.S. technology companies currently provide to the DHS as part of these engagements?
3. Please describe any non-confidential coordination between the DHS, U.S. technology companies, and other federal agencies that led to a federal enforcement action against an overseas scam compound or the foreign actors supporting the compound.
4. Please provide the DHS's total budget and current full-time equivalent staff dedicated to combating activity from overseas scam compounds.
5. What metrics, if any, does the DHS use to evaluate the effectiveness of its efforts to combat activity from overseas scam compounds? If the DHS plans to improve or develop these metrics, please describe how this will be achieved.
6. What dollar amount did the DHS help save or return to victims of activity from overseas scam compounds in Fiscal Year 2024 and Fiscal Year 2025 to date due to its efforts to combat these scams?
7. Please describe the DHS's coordination with the following entities to combat activity from overseas scam compounds. For each entity, identify the DHS offices involved; the scope and frequency of coordination; and any specific initiatives, joint operations, or information-sharing mechanisms:
  - a. Other U.S. federal agencies;
  - b. Foreign government or law enforcement agencies; and
  - c. International government or law enforcement agencies.
8. If the DHS plans to improve its current coordination activities related to the issues mentioned above, please describe how this will be achieved.
9. What additional tools, if any, would help aid the DHS in combating criminal scamming networks and the foreign actors supporting these networks?

Please provide your responses as soon as possible but in no event later than January 21, 2026. If you have any questions related to this request, please contact [REDACTED] of the Committee staff at [REDACTED] or [REDACTED]. Please send any official correspondence relating to this request to [REDACTED].



Sincerely,

A handwritten signature in blue ink, reading "David Schweikert".

---

David Schweikert  
Chairman

A handwritten signature in blue ink, reading "Eric S. Schmitt".

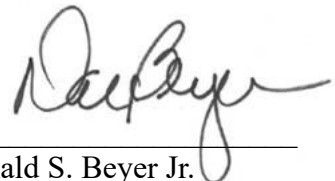
---

Eric S. Schmitt  
Vice Chairman

A handwritten signature in blue ink, reading "Margaret Wood Hassan".

---

Margaret Wood Hassan  
Ranking Member

A handwritten signature in blue ink, reading "Donald S. Beyer Jr.". The signature is stylized with a large "D" and "B".

---

Donald S. Beyer Jr.  
Senior House Democrat