

Congress of the United States
Washington, DC 20510

June 13, 2019

The Honorable Seema Verma
Administrator
Centers for Medicare and Medicaid Services
7500 Security Boulevard
Baltimore, MD 21244

Dear Administrator Verma:

We are writing today to provide you with the findings of a newly released Government Accountability Office (GAO) report identifying significant gaps in the Centers for Medicare and Medicaid Services' (CMS) protection of citizens' personally identifiable information (PII) that puts millions of individuals "at increased risk of identity fraud," and to ask that you act quickly to eliminate this vulnerability.

In 2017, Equifax Inc. – one of the nation's largest consumer reporting agencies (CRAs) - failed to protect its computer systems and consequently compromised to criminal hackers sensitive PII belonging to over 145 million Americans.¹ As part of the investigation of this breach, we learned that Equifax had numerous contracts with federal government agencies that collect and use PII, and we asked the GAO to conduct an investigation into the exposure and the effect the breach was likely to have on federal agencies and programs.²

The report, *Data Protection: Federal Agencies Need to Strengthen Online Identity Verification Processes*, which we are releasing today, identified a number of problems with at least four federal agencies' – including CMS – approach to protecting PII. Specifically, GAO found that CMS uses an outdated identity-proofing process that puts millions of Americans at risk – and does not have a plan to update that process to protect citizens from identity fraud.

CMS currently provides millions of Americans with online access to a federal health insurance marketplace – known as Healthcare.gov - where individuals can apply for Medicaid and private health insurance. Americans using Healthcare.gov to purchase health insurance deserve access to an online system that safeguards their PII. However, CMS uses an outdated process known as "knowledge-based verification" to verify the identity of individuals seeking to access this online portal. This process relies on questions generated by a CRA and typically asks

¹ Washington Post, "145 million Social Security numbers, 99 million addresses and more: Every type of personal data Equifax lost to hackers, by the numbers," Brian Fung, May 8, 2018, <https://www.washingtonpost.com/news/the-switch/wp/2018/05/08/every-type-of-personal-data-equifax-lost-to-hackers-by-the-numbers>

² Letter from Senator Elizabeth Warren to GAO, September 15, 2017, https://www.warren.senate.gov/files/documents/2017_09_15_GAO.pdf.

individuals looking to access the portal “questions derived from information found in their credit files, with the assumption that only the true owner of the identity would know the answers.”³

The GAO concluded that continued use of this process puts individuals “at increased risk of identity fraud,” and that “data stolen in recent breaches, such as the 2017 Equifax breach, could be used fraudulently” by individuals seeking to commit fraud.⁴ We are deeply troubled that you continued to use this flawed system even after the magnitude of the 2017 Equifax hack became clear. According to the GAO, you have not “implemented alternative methods” and “do not have a plan to reduce or eliminate the use of knowledge-based verification,” and as a result, “CMS and Healthcare.gov applicants will remain at an increased risk of identity fraud.”⁵ This is a disturbing conclusion, and I urge you to act quickly to address these concerns.

We ask that you answer the following questions and provide a briefing to our staff on this matter no later than June 27, 2019. And we ask you to develop and implement specific plans to improve your remote identity proofing processes and to protect citizens’ PII as soon as possible.

1. What steps did you take to protect consumer privacy following the 2017 Equifax data breach? Please describe any immediate actions taken as well as any long term operational changes that were implemented.
2. What policies do you have in place to ensure that third-parties it contracts with have appropriate data security practices?
3. The GAO study recommended that the Administrator of CMS should develop a plan with time frames and milestones to discontinue knowledge-based verification. The Department of Health and Human Services did not concur with this recommendation, because it felt existing alternatives were not suitable for certain populations served by CMS. Please provide estimates for the number of users who would be unable to utilize alternative verification methods and explain why a multifaceted approach to identity verification would be unsuitable. Will you commit to keeping our offices informed of your progress in this matter?
4. What alternative identity verification methods are currently under consideration by the CMS?
 - a. What is the specific schedule and timeline to have these plans fully implemented and in place for all individuals that rely on CMS’ online services?


Sincerely,

³ Government Accountability Office, “Data Protection: Federal Agencies Need to Strengthen Online Identity Verification Processes,” June 2019, <https://www.gao.gov/products/GAO-19-288>.

⁴ *Id.*

⁵ *Id.*


Elizabeth Warren
United States Senator


Ron Wyden
United States Senator


Elijah E. Cummings
Member of Congress

Congress of the United States
Washington, DC 20510

June 13, 2019

The Honorable Walter G. Copan
Director
National Institute of Standards and Technology
100 Bureau Drive
Gaithersburg, MD 20899

Dear Dr. Copan:

We are writing today to provide you with the findings of a newly released Government Accountability Office (GAO) report identifying significant gaps in the federal government's protection of citizens' personally identifiable information (PII), and to request information about how the National Institute of Standards and Technology (NIST) plans to provide appropriate guidance and assist federal agencies with their identity management processes in order to ensure this information is protected.

In 2017, Equifax Inc. – one of the nation's largest consumer reporting agencies (CRAs) - failed to protect its computer systems and consequently compromised to criminal hackers sensitive PII belonging to over 145 million Americans.¹ As part of the investigation of this breach, we learned that Equifax had numerous contracts with federal government agencies that collect and use PII, and we asked the Government Accountability Office (GAO) to conduct an investigation into the exposure and the effect the breach was likely to have on federal agencies and programs.²

The report, *Data Protection: Federal Agencies Need to Strengthen Online Identity Verification Processes*, which we are releasing today, reveals that the Equifax breach and other data breaches increased the risk that individuals that rely on government services from the Department of Veterans Affairs (VA), Centers for Medicaid and Medicare Services (CMS), the United States Postal Service (USPS), and the Social Security Administration (SSA) will suffer from identity fraud. GAO also revealed a need for NIST to issue a new guidance that would "assist federal agencies in determining and implementing alternatives" to an outdated identity verification process that "may put both the federal government and individuals at risk for fraud."³

¹ Washington Post, "145 million Social Security numbers, 99 million addresses and more: Every type of personal data Equifax lost to hackers, by the numbers," Brian Fung, May 8, 2018, <https://www.washingtonpost.com/news/the-switch/wp/2018/05/08/every-type-of-personal-data-equifax-lost-to-hackers-by-the-numbers>


² Letter from Senator Elizabeth Warren to GAO, September 15, 2017, https://www.warren.senate.gov/files/documents/2017_09_15_GAO.pdf.

³ Government Accountability Office, "Data Protection: Federal Agencies Need to Strengthen Online Identity Verification Processes," June 2019, <https://www.gao.gov/products/GAO-19-288>.

Specifically, the GAO found that the VA, CMS, SSA and USPS continue to rely on an outdated identity verification method – known as “knowledge-based verification.” The process relies on questions generated by a CRA and typically asks individuals looking to access the portal “questions derived from information found in their credit files, with the assumption that only the true owner of the identity would know the answers.” The GAO concluded that the continued use of this process puts individuals “at increased risk of identity fraud,” and “data stolen in recent breaches, such as the 2017 Equifax breach, could be used fraudulently” by individuals seeking to commit identity fraud against citizens that use the online services provided by these agencies.⁴

While the GAO acknowledged and used NIST’s technical guidance on remote identity proofing for this study, it also recommends that your agency issue “additional guidance to assist federal agencies in determining and implementing alternatives to knowledge-based verification that are most suitable for their applications.”⁵ We urge you to follow the GAO’s recommendation and request that you provide our offices with specific information and a specific timeline on how and when you will execute your responsibility to offer improved technical guidance needed by agencies so they can improve their efforts to prevent fraud.

Sincerely,



Elizabeth Warren
United States Senator



Ron Wyden
United States Senators



Elijah E. Cummings
Member of Congress

⁴ *Id.*

⁵ *Id.*

Congress of the United States
Washington, DC 20510

June 13, 2019

The Honorable Mick Mulvaney
Director
Office of Management and Budget
725 17th Street, NW
Washington, DC 20503

Dear Director Mulvaney:

We are writing today to provide you with the findings of a newly released Government Accountability Office (GAO) report identifying significant gaps in the federal government's protection of citizens' personally identifiable information (PII), and to request information about the failure of the Office of Management and Budget (OMB) to provide appropriate guidance and assist federal agencies with their identity management processes in order to ensure this information is protected.

In 2017, Equifax Inc. — one of the nation's largest consumer reporting agencies (CRAs) — failed to protect its computer systems and consequently compromised to criminal hackers sensitive PII belonging to over 145 million Americans.¹ As part of the investigation of this breach, we learned that Equifax had numerous contracts with federal government agencies that collect and use PII, and we asked the Government Accountability Office (GAO) to conduct an investigation into the exposure and the effect the breach was likely to have on federal agencies and programs.²

The report, *Data Protection: Federal Agencies Need to Strengthen Online Identity Verification Processes*, which we are releasing today, reveals that the Equifax breach and other data breaches increased the risk that individuals that rely on government services from the Department of Veterans Affairs (VA), Centers for Medicaid and Medicare Services (CMS), the United States Postal Service (USPS), and the Social Security Administration (SSA) will suffer from identity fraud. GAO also revealed significant failures by OMB, which has statutory "oversight authority over federal agency information security practices" under the Federal Information Security Modernization Act.³

Specifically, the GAO found that:

¹ Washington Post, "145 million Social Security numbers, 99 million addresses and more: Every type of personal data Equifax lost to hackers, by the numbers," Brian Fung, May 8, 2018, <https://www.washingtonpost.com/news/the-switch/wp/2018/05/08/every-type-of-personal-data-equifax-lost-to-hackers-by-the-numbers>


² Letter from Senator Elizabeth Warren to GAO, September 15, 2017, https://www.warren.senate.gov/files/documents/2017_09_15_GAO.pdf.

³ Department of Homeland Security, "Federal information Security Modernization Act," <https://www.dhs.gov/cisa/federal-information-security-modernization-act>.

- The VA continues to use an outdated identity verification process – known as “knowledge-based verification” for “certain categories of individuals” and has no “specific plans with time frames and milestones to eliminate” its use. The process relies on questions generated by a CRA and typically asks individuals looking to access the portal “questions derived from information found in their credit files, with the assumption that only the true owner of the identity would know the answers.” The GAO concluded that continued use of this process puts individuals “at increased risk of identity fraud.”⁴
- Two agencies — SSA and USPS — “have stated they intend to reduce or eliminate” knowledge-based verification from their processes, but “do not yet have specific plans for doing so.”
- CMS continues to rely on knowledge-based verification, “has not implemented alternative methods” and does not have any plans to do so.
- The continued use of this knowledge-based verification process puts individuals “at increased risk of identity fraud,” and “data stolen in recent breaches, such as the 2017 Equifax breach, could be used fraudulently” by individuals seeking to commit identity fraud against individuals that use VA, CMS, SSA, or USPS services.
- OMB is failing to provide adequate guidance. According to the GAO, while OMB has draft policy, the agency “has not issued guidance to agencies specifically on identity proofing,” and “does not require agency reporting on progress in implementing secure remote identity proofing processes.”⁵

It is disappointing that, almost two years after the massive 2017 Equifax data breach, OMB has failed to provide executive agencies with appropriate guidance needed to protect their personal information. We urge you to exercise that power and follow the GAO’s recommendation to “issue guidance requiring federal agencies to report on their progress in adopting secure identity proofing processes.”⁶ We also request that you provide our offices with specific information and a specific timeline on how and when you will execute your obligation to oversee these changes.

Sincerely,



Elizabeth Warren
United States Senator



Ron Wyden
United States Senator

⁴ Government Accountability Office, “Data Protection: Federal Agencies Need to Strengthen Online Identity Verification Processes,” June 2019, <https://www.gao.gov/products/GAO-19-288>.

⁵ *Id.*

⁶ *Id.*

Elijah E. Cummings

Elijah E. Cummings
Member of Congress

Congress of the United States
Washington, DC 20510

June 13, 2019

The Honorable Nancy Berryhill
Acting Commissioner
Social Security Administration
1100 West High Rise
6401 Security Blvd.
Baltimore, MD 21235

Dear Acting Commissioner Berryhill:

We are writing today to provide you with the findings of a newly released Government Accountability Office (GAO) report identifying significant gaps in the Social Security Administration's (SSA) protection of citizens' personally identifiable information (PII) that puts millions of individuals "at increased risk of identity fraud," and to ask that you act quickly to eliminate this vulnerability.

In 2017, Equifax Inc. — one of the nation's largest consumer reporting agencies (CRAs) — failed to protect its computer systems and consequently compromised to criminal hackers sensitive PII belonging to over 145 million Americans.¹ As part of the investigation of this breach, we learned that Equifax had numerous contracts with federal government agencies that collect and use PII, and we asked the GAO to conduct an investigation into the exposure and the effect the breach was likely to have on federal agencies and programs.²

The report, *Data Protection: Federal Agencies Need to Strengthen Online Identity Verification Processes*, which we are releasing today, identified a number of problems with the approach to protecting PII taken by at least four federal agencies' — including SSA. Specifically, GAO found that SSA uses an outdated identity-proofing process that puts millions of Americans at risk — and does "not yet have specific plans ... to reduce or eliminate" the use of this process.

SSA currently operates an online portal known as "My Social Security" where individuals can apply for retirement, disability, and Medicare benefits, request replacement Social Security and Medicare cards, set up direct deposits, and get a proof of income letter.³ However, SSA uses an outdated process known as "knowledge-based verification" to verify the

¹ Washington Post, "145 million Social Security numbers, 99 million addresses and more: Every type of personal data Equifax lost to hackers, by the numbers," Brian Fung, May 8, 2018, <https://www.washingtonpost.com/news/the-switch/wp/2018/05/08/every-type-of-personal-data-equifax-lost-to-hackers-by-the-numbers>

² Letter from Senator Elizabeth Warren to GAO, September 15, 2017, https://www.warren.senate.gov/files/documents/2017_09_15_GAO.pdf.

³ Social Security Administration, "Create your personal my Social Security account today," <https://www.ssa.gov/myaccount/>.

identity of individuals seeking to access this online portal. This process relies on questions generated by a CRA and typically asks individuals looking to access the portal “questions derived from information found in their credit files, with the assumption that only the true owner of the identity would know the answers.”⁴

The GAO concluded that continued use of this process puts individuals “at increased risk of identity fraud,” and that “data stolen in recent breaches, such as the 2017 Equifax breach, could be used fraudulently” by individuals seeking to commit fraud.⁵ We are deeply troubled that you continued to use this flawed system even after the magnitude of the 2017 Equifax hack became clear. You informed the GAO that you plan to “pilot alternative verification methods” and eliminate the outdated process by fiscal year 2020. However, according to the GAO, SSA “does not yet have specific plans and milestones to achieve its goal ... by fiscal year 2020,” and until you implement these plans, “the agency and the individuals that rely on its services will remain at an increased risk of identity fraud.”⁶ This is a disturbing conclusion, and I urge you to act quickly to address these concerns.

We ask that you answer the following questions and provide a briefing to our staff on this matter no later than June 27, 2019. And we ask you to develop and implement specific plans to improve your remote identity proofing processes and to protect citizens’ PII as soon as possible:


1. What steps did you take to protect consumer privacy following the 2017 Equifax data breach? Please describe any immediate actions taken as well as any long term operational changes that were implemented.
2. What policies do you have in place to ensure that third-parties SSA contracts with have appropriate data security practices?
3. The GAO study recommended that the Commissioner of Social Security should develop a plan with specific milestones to discontinue knowledge-based verification. SSA concurred with this recommendation. When will SSA complete this plan? If it is not possible to provide a timeline, please explain why. Will you commit to keeping our offices informed of your progress in this matter?
4. What alternative identity verification methods are currently under consideration by the SSA?
 - a. What is the specific schedule and timeline to have these plans fully implemented and in place for all SSA recipients?

⁴ Government Accountability Office, “Data Protection: Federal Agencies Need to Strengthen Online Identity Verification Processes,” June 2019, <https://www.gao.gov/products/GAO-19-288>.

⁵ *Id.*

⁶ *Id.*

Sincerely,



Elizabeth Warren
United States Senator



Ron Wyden
United States Senator



Elijah E. Cummings
Member of Congress

Congress of the United States
Washington, DC 20510

June 13, 2019

The Honorable Robert Wilkie
Secretary
Department of Veterans Affairs
810 Vermont Avenue, NW
Washington, DC 20420

Dear Secretary Wilkie:

We are writing today to provide you with the findings of a newly released Government Accountability Office (GAO) report identifying significant gaps in the Department of Veterans Affairs' (VA) protection of citizens' personally identifiable information (PII) that puts millions of individuals "at increased risk of identity fraud," and to ask that you act quickly to eliminate this vulnerability.

In 2017, Equifax Inc. — one of the nation's largest consumer reporting agencies (CRAs) — failed to protect its computer systems and consequently compromised to criminal hackers sensitive PII belonging to over 145 million Americans.¹ As part of the investigation of this breach, we learned that Equifax had numerous contracts with federal government agencies that collect and use PII, and we asked the GAO to conduct an investigation into the exposure and the effect the breach was likely to have on federal agencies and programs.²

The report, *Data Protection: Federal Agencies Need to Strengthen Online Identity Verification Processes*, which the approach to protecting PII taken by we are releasing today, identified a number of problems with at least four federal agencies' — including the VA's — approach to protecting PII. Specifically, GAO found that the VA continues to rely on an outdated identity-proofing process for some beneficiaries that puts their data at risk.

The VA currently "allows service members and veterans to apply for benefits using the agency's MyHealtheVet, VA.gov, and eBenefits systems." Although the VA has modified procedures, the agency still uses an outdated process known as "knowledge-based verification" to verify the identity of some individuals seeking to access these online portals. Specifically, GAO reported that while VA "has taken steps to enhance the effectiveness of their remote identify-proofing process," the agency has only "implemented alternative methods, but only as a supplement to the continued use of knowledge-based verification." This process relies on

¹ Washington Post, "145 million Social Security numbers, 99 million addresses and more: Every type of personal data Equifax lost to hackers, by the numbers," Brian Fung, May 8, 2018, <https://www.washingtonpost.com/news/the-switch/wp/2018/05/08/every-type-of-personal-data-equifax-lost-to-hackers-by-the-numbers>

² Letter from Senator Elizabeth Warren to GAO, September 15, 2017, https://www.warren.senate.gov/files/documents/2017_09_15_GAO.pdf.

questions generated by a CRA and typically asks individuals seeking to access the portal “questions derived from information found in their credit files, with the assumption that only the true owner of the identity would know the answers.”³

The GAO concluded that continued use of this process puts individuals “at increased risk of identity fraud,” and that “data stolen in recent breaches, such as the 2017 Equifax breach, could be used fraudulently” by individuals seeking to commit fraud.⁴ We are deeply troubled that you continued to use this flawed system even after the magnitude of the 2017 Equifax hack became clear. You informed the GAO that you have “implemented some alternative methods,” but according to GAO, the VA “does not have specific plans with time frames and milestones to eliminate” the outdated verification process, and until you develop them, “VA and the individuals it serves will continue to face a degree of identity fraud risk that could be reduced.”⁵ This is a disturbing conclusion, and I urge you to act quickly to address these concerns.

We ask that you answer the following questions and provide a briefing to our staff on this matter no later than June 27, 2019. And we ask you to develop and implement specific plans to improve your remote identity proofing processes and to protect citizens’ PII as soon as possible.

1. What steps did you take to protect consumer privacy following the 2017 Equifax data breach? Please describe any immediate actions taken as well as any long term operational changes that were implemented.
2. What policies do you have in place to ensure that third-parties the VA contracts with have appropriate data security practices?
3. The GAO study recommended that the Secretary of the Department of Veterans Affairs should develop a plan with time frames and milestones to discontinue knowledge-based verification. The VA concurred with this recommendation. When will the VA complete this plan? If it is not possible to provide a timeline, please explain why. Will you commit to keeping our offices informed of your progress in this matter?
4. What alternative identity verification methods are currently under consideration by the VA?
 - a. What is the specific schedule and timeline to have these plans fully implemented and in place for all individuals that rely on the VA’s online services?

³ Government Accountability Office, “Data Protection: Federal Agencies Need to Strengthen Online Identity Verification Processes,” June 2019, <https://www.gao.gov/products/GAO-19-288>.

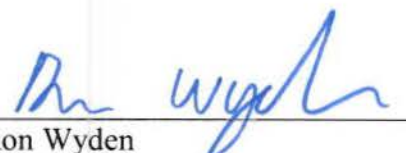
⁴ *Id.*

⁵ *Id.*

Sincerely,



Elizabeth Warren
United States Senator



Ron Wyden
United States Senator



Elijah E. Cummings
Member of Congress

Congress of the United States
Washington, DC 20510

June 13, 2019

The Honorable Megan J. Brennan
Postmaster General and Chief Executive Officer
United States Postal Service
475 L'Enfant Plaza, SW Room 4012
Washington, DC 20260-2200

Dear Postmaster General Brennan:

We are writing today to provide you with the findings of a newly released Government Accountability Office (GAO) report identifying significant gaps in the United States Postal Service's (USPS) protection of citizens' personally identifiable information (PII) that puts millions of individuals "at increased risk of identity fraud," and to ask that you act quickly to eliminate this vulnerability.

In 2017, Equifax Inc. — one of the nation's largest consumer reporting agencies (CRAs) — failed to protect its computer systems and consequently compromised to criminal hackers sensitive PII belonging to over 145 million Americans.¹ As part of the investigation of this breach, we learned that Equifax had numerous contracts with federal government agencies that collect and use PII, and we asked the GAO to conduct an investigation into the exposure and the effect the breach was likely to have on federal agencies and programs.²

The report, *Data Protection: Federal Agencies Need to Strengthen Online Identity Verification Processes*, which we are releasing today, identified a number of problems with the approach to protecting PII taken by at least four federal agencies' — including the USPS. Specifically, GAO found that USPS uses an outdated identity-proofing process that puts millions of Americans at risk — and does "not yet have specific plans ... to reduce or eliminate" the use of this process.

USPS currently provides an online service "known as 'Informed Delivery,' which allows individuals to digitally preview letter-sized mail and manage incoming packages." However, USPS uses an outdated process known as "knowledge-based verification" to verify the identity of individuals seeking to access this online portal. This process relies on questions generated by a CRA and typically asks individuals looking to access the portal "questions derived from

¹ Washington Post, "145 million Social Security numbers, 99 million addresses and more: Every type of personal data Equifax lost to hackers, by the numbers," Brian Fung, May 8, 2018, <https://www.washingtonpost.com/news/the-switch/wp/2018/05/08/every-type-of-personal-data-equifax-lost-to-hackers-by-the-numbers>

² Letter from Senator Elizabeth Warren to GAO, September 15, 2017, https://www.warren.senate.gov/files/documents/2017_09_15_GAO.pdf.

information found in their credit files, with the assumption that only the true owner of the identity would know the answers.”³

The GAO concluded that continued use of this process puts individuals “at increased risk of identity fraud,” and that “data stolen in recent breaches, such as the 2017 Equifax breach, could be used fraudulently” by individuals seeking to commit fraud.⁴ We are deeply troubled that you continued to use this flawed system even after the magnitude of the 2017 Equifax hack became clear. You informed the GAO that you plan to “implement alternative methods in the future,” but according to the GAO, USPS “does not yet have specific plans and milestones” for doing so. GAO concluded that until you implement the use of these alternative verification methods, “USPS and its customers will remain at increased risk of identity fraud.”⁵ This is a disturbing conclusion, and I urge you to act quickly to address these concerns.

We ask that you answer the following questions and provide a briefing to our staff on this matter no later than June 27, 2019. And we ask you to develop and implement specific plans to improve your remote identity proofing processes and to protect citizens’ PII as soon as possible.


1. What steps did you take to protect consumer privacy following the 2017 Equifax data breach? Please describe any immediate actions taken as well as any long term operational changes that were implemented.
2. What policies do you have in place to ensure that third-parties USPS contracts with have appropriate data security practices?
3. The GAO study recommended that the Postmaster General of the United States should complete a plan with time frames and milestones to discontinue knowledge-based verification. USPS concurred with this recommendation, and stated it planned to replace knowledge-based verification with mobile phone verification by December 2019. Does USPS anticipate a significant number of customers will be unable to be served using this method? Will you commit to keeping our offices informed of your progress in this matter?
4. What alternative identity verification methods are currently under consideration by the USPS?
 - a. What is the specific schedule and timeline to have these plans fully implemented and in place for all individuals that rely on USPS’s online services?

³ Government Accountability Office, “Data Protection: Federal Agencies Need to Strengthen Online Identity Verification Processes,” June 2019, <https://www.gao.gov/products/GAO-19-288>.

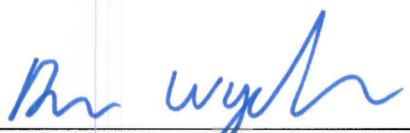
⁴ *Id.*

⁵ *Id.*

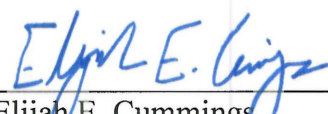
Sincerely,



Elizabeth Warren
United States Senator



Ron Wyden
United States Senator



Elijah E. Cummings
Member of Congress