Congress of the United States

Washington, DC 20515

November 23, 2026

Jimmy Roussel
Chief Executive Officer
IDScan.net
935 Gravier St.
New Orleans, LA 70112

Dear Mr. Roussel:

We write regarding highly concerning reports that over one hundred million Americans may have had personally identifying information (PII) stolen and sold on the dark web. While the Federal Bureau of Investigation is currently investigating the source of the data, this breach's scale warrants additional attention to the data-handling practices of companies like yours.

In September, cybersecurity researchers discovered "Nexus," an identity theft service on the dark web.[1] Nexus sold illegally obtained PII, including over 150 million American drivers licenses, nearly 600,000 medical cards, and other forms of PII such as employment authorizations, Common Access Cards, and travel documents at a large scale.[2] Nexus also offered PII of high-ranking American military and intelligence officials, and reports indicate other government employees were impacted.[3] According to reports, the data was "continuously" exfiltrated from a breach at a "major identity verification company," for months.[4] While reports indicate Nexus has since disappeared offline, the consequences of this theft may be widespread and persistent.

Remedying this kind of breach is extremely difficult, underscoring the importance of strong data security practices to prevent any such breach. If the reported extent of the breach is true, tens of millions of Americans' data have been exposed and are at risk of identity theft. This risk is further heightened by Nexus allegedly selling ultraviolet, infrared, and other detailed license images. Criminals can combine such PII with commercially available data to commit fraud or other crimes.[5] And foreign adversaries are likewise increasingly able to infer Americans' behavior though commercial data linked to government credentials.[6] Given the difficulty of

---

[1] Christine Hauser, "F.B.I. Investigates Sale of Millions of Stolen Driver's Licenses," *New York Times*, September 4, 2026, www.nytimes.com/2026/09/04/us/nexus-identity-theft-data-breach-fbi.html.

[2] Brian Krebs, "FBI Probes Service Selling 153M+ Drivers Licenses." *Krebs on Security*, September 1, 2026, https://krebsonsecurity.com/2026/09/fbi-probes-service-selling-153m-drivers-licenses/.

[3] Tom Uren, "America's Driver's License Breach Is a National Security Disaster," Lawfare, September 14, 2026, https://www.lawfaremedia.org/article/america%27s-drivers-licence-breach-is-a-national-security-disaster.

[4] Krebs, "FBI Probes Service Selling 153M+ Drivers Licenses."

[5] Jiahao Chen et al., "Profiling for Pennies: Unveiling the Privacy Iceberg of LLM Agents" (preprint, submitted May 7, 2026), arXiv:2605.06232, https://doi.org/10.48550/arXiv.2605.06232

[6] Jonathan Rozen, "How Mass Surveillance from Online Advertising puts Journalists at Risk" Committee to Protect Journalists, August 27, 2026, https://cpj.org/special-reports/how-mass-surveillance-from-online-advertising-puts-journalists-at-risk/.
Anna-Maria Gueorguieva et al., "Privacy Without Remedy: An Assessment of Data Broker Compliance with California Privacy Law" (preprint, May 20, 2026), https://arxiv.org/pdf/2605.21376; Raphael Satter, "US Military Personnel Are Being Targeted Using Location Data, Pentagon Letter Shows" Reuters, May 28, 2026, https://www.reuters.com/business/media-telecom/pentagon-says-us-military-personnel-are-reportedly-being-targeted-using-location-2026-05-28/.

tracking these credentials and data sales, remedying this breach will pose substantial challenges even where no further crime is committed.

The Nexus breach is only one of numerous incidents that place Americans' privacy at risk and hurt the economy.[7] Your duty to safeguard data is critical in light of AI-driven cyberattack capabilities, which may be utilized by cybercriminals for zero-day exploits.[8] Companies like yours should reduce these risks by employing zero-trust architectures, proactively examining vulnerabilities in their systems, and minimizing overall data exposure through limited retention, collection, and sharing of PII where possible.[9]

To better understand existing data-handling practices and risks around ID-verification, we respectfully request responses to the following questions by January 5, 2027.

1. Does your company adopt the following privacy principles for Americans whose identities are verified by your service? If so, what specific actions are taken to ensure these principles are followed?
    a. Data minimization;
    b. Use limitations;
    c. End-to-end security; and
    d. Consumer notice and transparency.
2. Do you sell or share any PII associated with identity verification to third-party organizations?
    a. If so, please identify which third-parties, including any parties in which you contact with, as well as the purpose of the transfer and/or sale.
    b. If so, what data associated with identity verification can third-party organizations access?
    c. In what circumstances, if any, are biometrics, genetics, or other sensitive documents retained by third-party organizations using your service?
    d. If applicable, is it made clear to screened individuals what PII is being shared with third-party organizations?
3. Please outline your retention schedule for individuals' PII.
    a. If any PII is retained, are consumers able to request deletion in a timely manner?
4. Is any PII from users stored in the cloud or a central location within your company or a third-party organization?
    a. If applicable, when using in-person scanners for IDs, is any PII sent off-device?
5. What insight, if any, do you have into how third-party organizations that use your service protect data of screened individuals?
    a. Do you impose data use restrictions on third-party organizations?
    b. Do you provide PII handling guidance to third-party organizations? If so, could you estimate the rate of compliance with this guidance?

---

[7] Erika Harrell and Alexandra Thompson, "Victims of Identity Theft," Bureau of Justice Statistics, October 2023, https://bjs.ojp.gov/media/document/70156; Rustam Jamilov, Hélène Rey, and Ahmed Tahoun, "The Anatomy of Cyber Risk," *Oxford University,* July 2026, https://users.ox.ac.uk/~econ0628/Cyber_Risk.pdf.

[8] Anthropic Threat Intelligence, Disrupting the First Reported AI-Orchestrated Cyber Espionage Campaign (San Francisco: Anthropic, November 13, 2025), https://www.anthropic.com/news/disrupting-AI-espionage.

[9] National Institute of Standards and Technology, NIST Privacy Framework: A Tool for Improving Privacy through Enterprise Risk Management, version 1.0 (Gaithersburg, MD: National Institute of Standards and Technology, January 16, 2020), https://doi.org/10.6028/NIST.CSWP.01162020.NIST.SP.800-207.pdf

b. Do you provide PII handling guidance to third-party organizations? If so, could you estimate the rate of compliance with this guidance?

6. What cybersecurity practices does your company adopt to protect sensitive PII?
   a. Are you participating in any partnerships to use AI technologies to identify cybersecurity vulnerabilities?
7. Has your company experienced a data breach related to government issued IDs in the past year?
   a. Have you or a third-party organization unintentionally exposed PII associated with verification attempts?
   b. If applicable, what was the source and size of the security incident?
   c. If applicable, did you report to CISA, Ic3, or other relevant government entities?
   d. If applicable, what steps did you take to aid and inform victims or third-party organizations?
   e. If you use physical ID scanners, how often are software or firmware updates provided, on average? Are there security audits for scanners?

We look forward to receiving your response. Thank you for your attention to this matter.

Sincerely,

Brian Schatz
United States Senator

Marsha Blackburn
United States Senator

Kweisi Mfume
Member of Congress

Katie Boyd Britt
United States Senator

Pete Sessions
Member of Congress

Andy Kim
United States Senator

Congress of the United States

Washington, DC 20515

November 23, 2026

Rick Song
Chief Executive Officer
Persona Identities, Inc.,
981 Mission Street #95
San Francisco CA 94103

Dear Mr. Song:

We write regarding highly concerning reports that over one hundred million Americans may have had personally identifying information (PII) stolen and sold on the dark web. While the Federal Bureau of Investigation is currently investigating the source of the data, this breach's scale warrants additional attention to the data-handling practices of companies like yours.

In September, cybersecurity researchers discovered "Nexus," an identity theft service on the dark web.[1] Nexus sold illegally obtained PII, including over 150 million American drivers licenses, nearly 600,000 medical cards, and other forms of PII such as employment authorizations, Common Access Cards, and travel documents at a large scale.[2] Nexus also offered PII of high-ranking American military and intelligence officials, and reports indicate other government employees were impacted.[3] According to reports, the data was "continuously" exfiltrated from a breach at a "major identity verification company," for months.[4] While reports indicate Nexus has since disappeared offline, the consequences of this theft may be widespread and persistent.

Remedying this kind of breach is extremely difficult, underscoring the importance of strong data security practices to prevent any such breach. If the reported extent of the breach is true, tens of millions of Americans' data have been exposed and are at risk of identity theft. This risk is further heightened by Nexus allegedly selling ultraviolet, infrared, and other detailed license images. Criminals can combine such PII with commercially available data to commit fraud or other crimes.[5] And foreign adversaries are likewise increasingly able to infer Americans' behavior though commercial data linked to government credentials.[6] Given the difficulty of

---

[1] Christine Hauser, "F.B.I. Investigates Sale of Millions of Stolen Driver's Licenses," *New York Times*, September 4, 2026, www.nytimes.com/2026/09/04/us/nexus-identity-theft-data-breach-fbi.html.

[2] Brian Krebs, "FBI Probes Service Selling 153M+ Drivers Licenses." *Krebs on Security*, September 1, 2026, https://krebsonsecurity.com/2026/09/fbi-probes-service-selling-153m-drivers-licenses/.

[3] Tom Uren, "America's Driver's License Breach Is a National Security Disaster," Lawfare, September 14, 2026, https://www.lawfaremedia.org/article/america%27s-drivers-licence-breach-is-a-national-security-disaster.

[4] Krebs, "FBI Probes Service Selling 153M+ Drivers Licenses."

[5] Jiahao Chen et al., "Profiling for Pennies: Unveiling the Privacy Iceberg of LLM Agents" (preprint, submitted May 7, 2026), arXiv:2605.06232, https://doi.org/10.48550/arXiv.2605.06232

[6] Jonathan Rozen, "How Mass Surveillance from Online Advertising puts Journalists at Risk" Committee to Protect Journalists, August 27, 2026, https://cpj.org/special-reports/how-mass-surveillance-from-online-advertising-puts-journalists-at-risk/.
Anna-Maria Gueorguieva et al., "Privacy Without Remedy: An Assessment of Data Broker Compliance with California Privacy Law" (preprint, May 20, 2026), https://arxiv.org/pdf/2605.21376; Raphael Satter, "US Military Personnel Are Being Targeted Using Location Data, Pentagon Letter Shows" Reuters, May 28, 2026, https://www.reuters.com/business/media-telecom/pentagon-says-us-military-personnel-are-reportedly-being-targeted-using-location-2026-05-28/.

tracking these credentials and data sales, remedying this breach will pose substantial challenges even where no further crime is committed.

The Nexus breach is only one of numerous incidents that place Americans' privacy at risk and hurt the economy.[7] Your duty to safeguard data is critical in light of AI-driven cyberattack capabilities, which may be utilized by cybercriminals for zero-day exploits.[8] Companies like yours should reduce these risks by employing zero-trust architectures, proactively examining vulnerabilities in their systems, and minimizing overall data exposure through limited retention, collection, and sharing of PII where possible.[9]

To better understand existing data-handling practices and risks around ID-verification, we respectfully request responses to the following questions by January 5, 2027.

1. Does your company adopt the following privacy principles for Americans whose identities are verified by your service? If so, what specific actions are taken to ensure these principles are followed?
    a. Data minimization;
    b. Use limitations;
    c. End-to-end security; and
    d. Consumer notice and transparency.
2. Do you sell or share any PII associated with identity verification to third-party organizations?
    a. If so, please identify which third-parties, including any parties in which you contact with, as well as the purpose of the transfer and/or sale.
    b. If so, what data associated with identity verification can third-party organizations access?
    c. In what circumstances, if any, are biometrics, genetics, or other sensitive documents retained by third-party organizations using your service?
    d. If applicable, is it made clear to screened individuals what PII is being shared with third-party organizations?
3. Please outline your retention schedule for individuals' PII.
    a. If any PII is retained, are consumers able to request deletion in a timely manner?
4. Is any PII from users stored in the cloud or a central location within your company or a third-party organization?
    a. If applicable, when using in-person scanners for IDs, is any PII sent off-device?
5. What insight, if any, do you have into how third-party organizations that use your service protect data of screened individuals?
    a. Do you impose data use restrictions on third-party organizations?
    b. Do you provide PII handling guidance to third-party organizations? If so, could you estimate the rate of compliance with this guidance?

---

[7] Erika Harrell and Alexandra Thompson, "Victims of Identity Theft," Bureau of Justice Statistics, October 2023, https://bjs.ojp.gov/media/document/70156; Rustam Jamilov, Hélène Rey, and Ahmed Tahoun, "The Anatomy of Cyber Risk," *Oxford University,* July 2026, https://users.ox.ac.uk/~econ0628/Cyber_Risk.pdf.

[8] Anthropic Threat Intelligence, Disrupting the First Reported AI-Orchestrated Cyber Espionage Campaign (San Francisco: Anthropic, November 13, 2025), https://www.anthropic.com/news/disrupting-AI-espionage.

[9] National Institute of Standards and Technology, NIST Privacy Framework: A Tool for Improving Privacy through Enterprise Risk Management, version 1.0 (Gaithersburg, MD: National Institute of Standards and Technology, January 16, 2020), https://doi.org/10.6028/NIST.CSWP.01162020.NIST.SP.800-207.pdf

b. Do you provide PII handling guidance to third-party organizations? If so, could you estimate the rate of compliance with this guidance?

6. What cybersecurity practices does your company adopt to protect sensitive PII?
   a. Are you participating in any partnerships to use AI technologies to identify cybersecurity vulnerabilities?
7. Has your company experienced a data breach related to government issued IDs in the past year?
   a. Have you or a third-party organization unintentionally exposed PII associated with verification attempts?
   b. If applicable, what was the source and size of the security incident?
   c. If applicable, did you report to CISA, Ic3, or other relevant government entities?
   d. If applicable, what steps did you take to aid and inform victims or third-party organizations?
   e. If you use physical ID scanners, how often are software or firmware updates provided, on average? Are there security audits for scanners?

We look forward to receiving your response. Thank you for your attention to this matter.

Sincerely,

Brian Schatz
United States Senator

Marsha Blackburn
United States Senator

Kweisi Mfume
Member of Congress

Katie Boyd Britt
United States Senator

Pete Sessions
Member of Congress

Andy Kim
United States Senator

Congress of the United States

Washington, DC 20515

November 23, 2026

Caryn Seidman-Becker
Chief Executive Officer
Clear Secure, Inc.
85 10th Avenue
New York, NY 10011

Dear Ms. Seidman-Becker:

We write regarding highly concerning reports that over one hundred million Americans may have had personally identifying information (PII) stolen and sold on the dark web. While the Federal Bureau of Investigation is currently investigating the source of the data, this breach's scale warrants additional attention to the data-handling practices of companies like yours.

In September, cybersecurity researchers discovered "Nexus," an identity theft service on the dark web.[1] Nexus sold illegally obtained PII, including over 150 million American drivers licenses, nearly 600,000 medical cards, and other forms of PII such as employment authorizations, Common Access Cards, and travel documents at a large scale.[2] Nexus also offered PII of high-ranking American military and intelligence officials, and reports indicate other government employees were impacted.[3] According to reports, the data was "continuously" exfiltrated from a breach at a "major identity verification company," for months.[4] While reports indicate Nexus has since disappeared offline, the consequences of this theft may be widespread and persistent.

Remedying this kind of breach is extremely difficult, underscoring the importance of strong data security practices to prevent any such breach. If the reported extent of the breach is true, tens of millions of Americans' data have been exposed and are at risk of identity theft. This risk is further heightened by Nexus allegedly selling ultraviolet, infrared, and other detailed license images. Criminals can combine such PII with commercially available data to commit fraud or other crimes.[5] And foreign adversaries are likewise increasingly able to infer Americans' behavior though commercial data linked to government credentials.[6] Given the difficulty of

---

[1] Christine Hauser, "F.B.I. Investigates Sale of Millions of Stolen Driver's Licenses," *New York Times*, September 4, 2026, www.nytimes.com/2026/09/04/us/nexus-identity-theft-data-breach-fbi.html.

[2] Brian Krebs, "FBI Probes Service Selling 153M+ Drivers Licenses." *Krebs on Security*, September 1, 2026, https://krebsonsecurity.com/2026/09/fbi-probes-service-selling-153m-drivers-licenses/.

[3] Tom Uren, "America's Driver's License Breach Is a National Security Disaster," Lawfare, September 14, 2026, https://www.lawfaremedia.org/article/america%27s-drivers-licence-breach-is-a-national-security-disaster.

[4] Krebs, "FBI Probes Service Selling 153M+ Drivers Licenses."

[5] Jiahao Chen et al., "Profiling for Pennies: Unveiling the Privacy Iceberg of LLM Agents" (preprint, submitted May 7, 2026), arXiv:2605.06232, https://doi.org/10.48550/arXiv.2605.06232

[6] Jonathan Rozen, "How Mass Surveillance from Online Advertising puts Journalists at Risk" Committee to Protect Journalists, August 27, 2026, https://cpj.org/special-reports/how-mass-surveillance-from-online-advertising-puts-journalists-at-risk/.
Anna-Maria Gueorguieva et al., "Privacy Without Remedy: An Assessment of Data Broker Compliance with California Privacy Law" (preprint, May 20, 2026), https://arxiv.org/pdf/2605.21376; Raphael Satter, "US Military Personnel Are Being Targeted Using Location Data, Pentagon Letter Shows" Reuters, May 28, 2026, https://www.reuters.com/business/media-telecom/pentagon-says-us-military-personnel-are-reportedly-being-targeted-using-location-2026-05-28/.

tracking these credentials and data sales, remedying this breach will pose substantial challenges even where no further crime is committed.

The Nexus breach is only one of numerous incidents that place Americans' privacy at risk and hurt the economy.[7] Your duty to safeguard data is critical in light of AI-driven cyberattack capabilities, which may be utilized by cybercriminals for zero-day exploits.[8] Companies like yours should reduce these risks by employing zero-trust architectures, proactively examining vulnerabilities in their systems, and minimizing overall data exposure through limited retention, collection, and sharing of PII where possible.[9]

To better understand existing data-handling practices and risks around ID-verification, we respectfully request responses to the following questions by January 5, 2027.

1. Does your company adopt the following privacy principles for Americans whose identities are verified by your service? If so, what specific actions are taken to ensure these principles are followed?
    a. Data minimization;
    b. Use limitations;
    c. End-to-end security; and
    d. Consumer notice and transparency.
2. Do you sell or share any PII associated with identity verification to third-party organizations?
    a. If so, please identify which third-parties, including any parties in which you contact with, as well as the purpose of the transfer and/or sale.
    b. If so, what data associated with identity verification can third-party organizations access?
    c. In what circumstances, if any, are biometrics, genetics, or other sensitive documents retained by third-party organizations using your service?
    d. If applicable, is it made clear to screened individuals what PII is being shared with third-party organizations?
3. Please outline your retention schedule for individuals' PII.
    a. If any PII is retained, are consumers able to request deletion in a timely manner?
4. Is any PII from users stored in the cloud or a central location within your company or a third-party organization?
    a. If applicable, when using in-person scanners for IDs, is any PII sent off-device?
5. What insight, if any, do you have into how third-party organizations that use your service protect data of screened individuals?
    a. Do you impose data use restrictions on third-party organizations?
    b. Do you provide PII handling guidance to third-party organizations? If so, could you estimate the rate of compliance with this guidance?

---

[7] Erika Harrell and Alexandra Thompson, "Victims of Identity Theft," Bureau of Justice Statistics, October 2023, https://bjs.ojp.gov/media/document/70156; Rustam Jamilov, Hélène Rey, and Ahmed Tahoun, "The Anatomy of Cyber Risk," *Oxford University,* July 2026, https://users.ox.ac.uk/~econ0628/Cyber_Risk.pdf.

[8] Anthropic Threat Intelligence, Disrupting the First Reported AI-Orchestrated Cyber Espionage Campaign (San Francisco: Anthropic, November 13, 2025), https://www.anthropic.com/news/disrupting-AI-espionage.

[9] National Institute of Standards and Technology, NIST Privacy Framework: A Tool for Improving Privacy through Enterprise Risk Management, version 1.0 (Gaithersburg, MD: National Institute of Standards and Technology, January 16, 2020), https://doi.org/10.6028/NIST.CSWP.01162020.NIST.SP.800-207.pdf

b. Do you provide PII handling guidance to third-party organizations? If so, could you estimate the rate of compliance with this guidance?

6. What cybersecurity practices does your company adopt to protect sensitive PII?
   a. Are you participating in any partnerships to use AI technologies to identify cybersecurity vulnerabilities?
7. Has your company experienced a data breach related to government issued IDs in the past year?
   a. Have you or a third-party organization unintentionally exposed PII associated with verification attempts?
   b. If applicable, what was the source and size of the security incident?
   c. If applicable, did you report to CISA, Ic3, or other relevant government entities?
   d. If applicable, what steps did you take to aid and inform victims or third-party organizations?
   e. If you use physical ID scanners, how often are software or firmware updates provided, on average? Are there security audits for scanners?

We look forward to receiving your response. Thank you for your attention to this matter.

Sincerely,

Brian Schatz
United States Senator

Marsha Blackburn
United States Senator

Kweisi Mfume
Member of Congress

Katie Boyd Britt
United States Senator

Pete Sessions
Member of Congress

Andy Kim
United States Senator

Congress of the United States

Washington, DC 20515

November 23, 2026

Brian Lewis
Chief Executive Officer
Intellicheck, Inc.
200 Broadhollow Road, #207
Melville NY 11747

Dear Mr. Lewis:

We write regarding highly concerning reports that over one hundred million Americans may have had personally identifying information (PII) stolen and sold on the dark web. While the Federal Bureau of Investigation is currently investigating the source of the data, this breach's scale warrants additional attention to the data-handling practices of companies like yours.

In September, cybersecurity researchers discovered "Nexus," an identity theft service on the dark web.[1] Nexus sold illegally obtained PII, including over 150 million American drivers licenses, nearly 600,000 medical cards, and other forms of PII such as employment authorizations, Common Access Cards, and travel documents at a large scale.[2] Nexus also offered PII of high-ranking American military and intelligence officials, and reports indicate other government employees were impacted.[3] According to reports, the data was "continuously" exfiltrated from a breach at a "major identity verification company," for months.[4] While reports indicate Nexus has since disappeared offline, the consequences of this theft may be widespread and persistent.

Remedying this kind of breach is extremely difficult, underscoring the importance of strong data security practices to prevent any such breach. If the reported extent of the breach is true, tens of millions of Americans' data have been exposed and are at risk of identity theft. This risk is further heightened by Nexus allegedly selling ultraviolet, infrared, and other detailed license images. Criminals can combine such PII with commercially available data to commit fraud or other crimes.[5] And foreign adversaries are likewise increasingly able to infer Americans' behavior though commercial data linked to government credentials.[6] Given the difficulty of

---

[1] Christine Hauser, "F.B.I. Investigates Sale of Millions of Stolen Driver's Licenses," *New York Times*, September 4, 2026, www.nytimes.com/2026/09/04/us/nexus-identity-theft-data-breach-fbi.html.

[2] Brian Krebs, "FBI Probes Service Selling 153M+ Drivers Licenses." *Krebs on Security*, September 1, 2026, https://krebsonsecurity.com/2026/09/fbi-probes-service-selling-153m-drivers-licenses/.

[3] Tom Uren, "America's Driver's License Breach Is a National Security Disaster," Lawfare, September 14, 2026, https://www.lawfaremedia.org/article/america%27s-drivers-licence-breach-is-a-national-security-disaster.

[4] Krebs, "FBI Probes Service Selling 153M+ Drivers Licenses."

[5] Jiahao Chen et al., "Profiling for Pennies: Unveiling the Privacy Iceberg of LLM Agents" (preprint, submitted May 7, 2026), arXiv:2605.06232, https://doi.org/10.48550/arXiv.2605.06232

[6] Jonathan Rozen, "How Mass Surveillance from Online Advertising puts Journalists at Risk" Committee to Protect Journalists, August 27, 2026, https://cpj.org/special-reports/how-mass-surveillance-from-online-advertising-puts-journalists-at-risk/.
Anna-Maria Gueorguieva et al., "Privacy Without Remedy: An Assessment of Data Broker Compliance with California Privacy Law" (preprint, May 20, 2026), https://arxiv.org/pdf/2605.21376; Raphael Satter, "US Military Personnel Are Being Targeted Using Location Data, Pentagon Letter Shows" Reuters, May 28, 2026, https://www.reuters.com/business/media-telecom/pentagon-says-us-military-personnel-are-reportedly-being-targeted-using-location-2026-05-28/.

tracking these credentials and data sales, remedying this breach will pose substantial challenges even where no further crime is committed.

The Nexus breach is only one of numerous incidents that place Americans' privacy at risk and hurt the economy.[7] Your duty to safeguard data is critical in light of AI-driven cyberattack capabilities, which may be utilized by cybercriminals for zero-day exploits.[8] Companies like yours should reduce these risks by employing zero-trust architectures, proactively examining vulnerabilities in their systems, and minimizing overall data exposure through limited retention, collection, and sharing of PII where possible.[9]

To better understand existing data-handling practices and risks around ID-verification, we respectfully request responses to the following questions by January 5, 2027.

1. Does your company adopt the following privacy principles for Americans whose identities are verified by your service? If so, what specific actions are taken to ensure these principles are followed?
    a. Data minimization;
    b. Use limitations;
    c. End-to-end security; and
    d. Consumer notice and transparency.
2. Do you sell or share any PII associated with identity verification to third-party organizations?
    a. If so, please identify which third-parties, including any parties in which you contact with, as well as the purpose of the transfer and/or sale.
    b. If so, what data associated with identity verification can third-party organizations access?
    c. In what circumstances, if any, are biometrics, genetics, or other sensitive documents retained by third-party organizations using your service?
    d. If applicable, is it made clear to screened individuals what PII is being shared with third-party organizations?
3. Please outline your retention schedule for individuals' PII.
    a. If any PII is retained, are consumers able to request deletion in a timely manner?
4. Is any PII from users stored in the cloud or a central location within your company or a third-party organization?
    a. If applicable, when using in-person scanners for IDs, is any PII sent off-device?
5. What insight, if any, do you have into how third-party organizations that use your service protect data of screened individuals?
    a. Do you impose data use restrictions on third-party organizations?
    b. Do you provide PII handling guidance to third-party organizations? If so, could you estimate the rate of compliance with this guidance?

---

[7] Erika Harrell and Alexandra Thompson, "Victims of Identity Theft," Bureau of Justice Statistics, October 2023, https://bjs.ojp.gov/media/document/70156; Rustam Jamilov, Hélène Rey, and Ahmed Tahoun, "The Anatomy of Cyber Risk," *Oxford University,* July 2026, https://users.ox.ac.uk/~econ0628/Cyber_Risk.pdf.

[8] Anthropic Threat Intelligence, Disrupting the First Reported AI-Orchestrated Cyber Espionage Campaign (San Francisco: Anthropic, November 13, 2025), https://www.anthropic.com/news/disrupting-AI-espionage.

[9] National Institute of Standards and Technology, NIST Privacy Framework: A Tool for Improving Privacy through Enterprise Risk Management, version 1.0 (Gaithersburg, MD: National Institute of Standards and Technology, January 16, 2020), https://doi.org/10.6028/NIST.CSWP.01162020.NIST.SP.800-207.pdf

b. Do you provide PII handling guidance to third-party organizations? If so, could you estimate the rate of compliance with this guidance?

6. What cybersecurity practices does your company adopt to protect sensitive PII?
   a. Are you participating in any partnerships to use AI technologies to identify cybersecurity vulnerabilities?
7. Has your company experienced a data breach related to government issued IDs in the past year?
   a. Have you or a third-party organization unintentionally exposed PII associated with verification attempts?
   b. If applicable, what was the source and size of the security incident?
   c. If applicable, did you report to CISA, Ic3, or other relevant government entities?
   d. If applicable, what steps did you take to aid and inform victims or third-party organizations?
   e. If you use physical ID scanners, how often are software or firmware updates provided, on average? Are there security audits for scanners?

We look forward to receiving your response. Thank you for your attention to this matter.

Sincerely,

Brian Schatz
United States Senator

Marsha Blackburn
United States Senator

Kweisi Mfume
Member of Congress

Katie Boyd Britt
United States Senator

Pete Sessions
Member of Congress

Andy Kim
United States Senator

Congress of the United States

Washington, DC 20515

November 23, 2026

Blake Hall
Chief Executive Officer
ID.me
8261 Greensboro Drive, Suite 600
McLean VA 22102

Dear Mr. Hall:

We write regarding highly concerning reports that over one hundred million Americans may have had personally identifying information (PII) stolen and sold on the dark web. While the Federal Bureau of Investigation is currently investigating the source of the data, this breach's scale warrants additional attention to the data-handling practices of companies like yours.

In September, cybersecurity researchers discovered "Nexus," an identity theft service on the dark web.[1] Nexus sold illegally obtained PII, including over 150 million American drivers licenses, nearly 600,000 medical cards, and other forms of PII such as employment authorizations, Common Access Cards, and travel documents at a large scale.[2] Nexus also offered PII of high-ranking American military and intelligence officials, and reports indicate other government employees were impacted.[3] According to reports, the data was "continuously" exfiltrated from a breach at a "major identity verification company," for months.[4] While reports indicate Nexus has since disappeared offline, the consequences of this theft may be widespread and persistent.

Remedying this kind of breach is extremely difficult, underscoring the importance of strong data security practices to prevent any such breach. If the reported extent of the breach is true, tens of millions of Americans' data have been exposed and are at risk of identity theft. This risk is further heightened by Nexus allegedly selling ultraviolet, infrared, and other detailed license images. Criminals can combine such PII with commercially available data to commit fraud or other crimes.[5] And foreign adversaries are likewise increasingly able to infer Americans' behavior though commercial data linked to government credentials.[6] Given the difficulty of

---

[1] Christine Hauser, "F.B.I. Investigates Sale of Millions of Stolen Driver's Licenses," *New York Times*, September 4, 2026, www.nytimes.com/2026/09/04/us/nexus-identity-theft-data-breach-fbi.html.

[2] Brian Krebs, "FBI Probes Service Selling 153M+ Drivers Licenses." *Krebs on Security*, September 1, 2026, https://krebsonsecurity.com/2026/09/fbi-probes-service-selling-153m-drivers-licenses/.

[3] Tom Uren, "America's Driver's License Breach Is a National Security Disaster," Lawfare, September 14, 2026, https://www.lawfaremedia.org/article/america%27s-drivers-licence-breach-is-a-national-security-disaster.

[4] Krebs, "FBI Probes Service Selling 153M+ Drivers Licenses."

[5] Jiahao Chen et al., "Profiling for Pennies: Unveiling the Privacy Iceberg of LLM Agents" (preprint, submitted May 7, 2026), arXiv:2605.06232, https://doi.org/10.48550/arXiv.2605.06232

[6] Jonathan Rozen, "How Mass Surveillance from Online Advertising puts Journalists at Risk" Committee to Protect Journalists, August 27, 2026, https://cpj.org/special-reports/how-mass-surveillance-from-online-advertising-puts-journalists-at-risk/.
Anna-Maria Gueorguieva et al., "Privacy Without Remedy: An Assessment of Data Broker Compliance with California Privacy Law" (preprint, May 20, 2026), https://arxiv.org/pdf/2605.21376; Raphael Satter, "US Military Personnel Are Being Targeted Using Location Data, Pentagon Letter Shows" Reuters, May 28, 2026, https://www.reuters.com/business/media-telecom/pentagon-says-us-military-personnel-are-reportedly-being-targeted-using-location-2026-05-28/.

tracking these credentials and data sales, remedying this breach will pose substantial challenges even where no further crime is committed.

The Nexus breach is only one of numerous incidents that place Americans' privacy at risk and hurt the economy.[7] Your duty to safeguard data is critical in light of AI-driven cyberattack capabilities, which may be utilized by cybercriminals for zero-day exploits.[8] Companies like yours should reduce these risks by employing zero-trust architectures, proactively examining vulnerabilities in their systems, and minimizing overall data exposure through limited retention, collection, and sharing of PII where possible.[9]

To better understand existing data-handling practices and risks around ID-verification, we respectfully request responses to the following questions by January 5, 2027.

1. Does your company adopt the following privacy principles for Americans whose identities are verified by your service? If so, what specific actions are taken to ensure these principles are followed?
    a. Data minimization;
    b. Use limitations;
    c. End-to-end security; and
    d. Consumer notice and transparency.
2. Do you sell or share any PII associated with identity verification to third-party organizations?
    a. If so, please identify which third-parties, including any parties in which you contact with, as well as the purpose of the transfer and/or sale.
    b. If so, what data associated with identity verification can third-party organizations access?
    c. In what circumstances, if any, are biometrics, genetics, or other sensitive documents retained by third-party organizations using your service?
    d. If applicable, is it made clear to screened individuals what PII is being shared with third-party organizations?
3. Please outline your retention schedule for individuals' PII.
    a. If any PII is retained, are consumers able to request deletion in a timely manner?
4. Is any PII from users stored in the cloud or a central location within your company or a third-party organization?
    a. If applicable, when using in-person scanners for IDs, is any PII sent off-device?
5. What insight, if any, do you have into how third-party organizations that use your service protect data of screened individuals?
    a. Do you impose data use restrictions on third-party organizations?
    b. Do you provide PII handling guidance to third-party organizations? If so, could you estimate the rate of compliance with this guidance?

---

[7] Erika Harrell and Alexandra Thompson, "Victims of Identity Theft," Bureau of Justice Statistics, October 2023, https://bjs.ojp.gov/media/document/70156; Rustam Jamilov, Hélène Rey, and Ahmed Tahoun, "The Anatomy of Cyber Risk," *Oxford University,* July 2026, https://users.ox.ac.uk/~econ0628/Cyber_Risk.pdf.

[8] Anthropic Threat Intelligence, Disrupting the First Reported AI-Orchestrated Cyber Espionage Campaign (San Francisco: Anthropic, November 13, 2025), https://www.anthropic.com/news/disrupting-AI-espionage.

[9] National Institute of Standards and Technology, NIST Privacy Framework: A Tool for Improving Privacy through Enterprise Risk Management, version 1.0 (Gaithersburg, MD: National Institute of Standards and Technology, January 16, 2020), https://doi.org/10.6028/NIST.CSWP.01162020.NIST.SP.800-207.pdf

b. Do you provide PII handling guidance to third-party organizations? If so, could you estimate the rate of compliance with this guidance?

6. What cybersecurity practices does your company adopt to protect sensitive PII?
   a. Are you participating in any partnerships to use AI technologies to identify cybersecurity vulnerabilities?
7. Has your company experienced a data breach related to government issued IDs in the past year?
   a. Have you or a third-party organization unintentionally exposed PII associated with verification attempts?
   b. If applicable, what was the source and size of the security incident?
   c. If applicable, did you report to CISA, Ic3, or other relevant government entities?
   d. If applicable, what steps did you take to aid and inform victims or third-party organizations?
   e. If you use physical ID scanners, how often are software or firmware updates provided, on average? Are there security audits for scanners?

We look forward to receiving your response. Thank you for your attention to this matter.

Sincerely,

Brian Schatz
United States Senator

Marsha Blackburn
United States Senator

Kweisi Mfume
Member of Congress

Katie Boyd Britt
United States Senator

Pete Sessions
Member of Congress

Andy Kim
United States Senator