

United States Senate

WASHINGTON, DC 20510

December 12, 2019

Mark W. Begor
Chief Executive Officer
Equifax Inc.
1550 Peachtree St NW
Atlanta, GA 30309

Dear Mr. Begor:

We write with alarm about your company's failure to provide transparency into your receipt, handling, and reporting of consumer information through national security letters (NSLs) from the Federal Bureau of Investigation (FBI). NSLs are akin to administrative subpoenas that require the recipient to divulge information that the FBI deems relevant to national security investigations, including sensitive information on the company's consumers, including names, addresses, billing records, and even full credit reports. The FBI can send NSLs without gaining prior approval from a judge.^{1,2}

In September, the Electronic Frontier Foundation released a large set of documents gained via a Freedom of Information Act lawsuit indicating that credit reporting agencies such as yours have frequently been the recipients of NSLs, a fact which previously was not publicly known.³

As one of the three credit reporting agencies in the US, your company collects and sells credit information on vast numbers of Americans. Equifax has information on at least 145.5 million US consumers.⁴ Because your company holds so much potentially sensitive data on so many Americans and collects this information without obtaining consent from these individuals, you have a responsibility to protect individuals' data and be transparent about how or when you disclose it. Unfortunately, your company has not provided information to policymakers or the public about the type or the number of disclosures that you have made to the FBI.

The USA FREEDOM Act was intended, in part, to increase the level of transparency around NSLs. Section 603 of the Act specifically permits entities that receive NSLs to report aggregated

¹ New York Times, "Secret F.B.I. Subpoenas Scoop Up Personal Data From Scores of Companies," Jennifer Valentino-DeVries, September 20, 2019. <https://www.nytimes.com/2019/09/20/us/data-privacy-fbi.html>.

² Congressional Research Service, "National Security Letters in Foreign Intelligence Investigations: Legal Background," Charles Doyle, July 30, 2015, <https://fas.org/sgp/crs/intel/RL33320.pdf>.

³ New York Times, "Secret F.B.I. Subpoenas Scoop Up Personal Data From Scores of Companies," Jennifer Valentino-DeVries, September 20, 2019. <https://www.nytimes.com/2019/09/20/us/data-privacy-fbi.html>.

⁴ Equifax Inc., "2018 Annual Report," February 21, 2019, p. 15, <https://investor.equifax.com/~media/Files/E/Equifax-IR/Annual%20Reports/2018-annual-report.pdf>.

information about them, including the number of NSLs received.⁵ Dozens of technology and telecommunication companies publish reports of statistics about their receipt of NSLs.⁶ But Equifax maintains no such publicly available information and has not provided information about NSL receipt when asked by reporters.⁷

NSLs are typically accompanied by nondisclosure orders that prevent recipients from disclosing that they have received the letter. Section 502(f) of the Act requires the government to periodically review these nondisclosure orders and determine whether the orders can be terminated. It also requires the government to send notification, in the form of a so-called “termination letter,” to NSL recipients if and when the nondisclosure order is terminated. This allows the recipient to speak.⁸ Some companies routinely publish NSLs upon their receipt of termination letters.⁹

The records disclosed by the Electronic Frontier Foundation show that Equifax has received dozens of termination letters from the FBI that terminate NSL nondisclosure orders.¹⁰ Yet, although it is no longer barred from discussing those NSLs, your company has not published anything about them. Such publications give the public a sense of the content that companies share with the FBI. American consumers deserve to know what happens to the data that your company collects, which can encompass all of the major financial relationships that a consumer might have over the course of their lifetime.

To provide clarity about how your company provides sensitive consumer financial data to the government, we ask that you answer the following questions no later than December 27, 2019.

⁵ USA FREEDOM Act of 2015, H.R. 2048, 114th Cong., § 603(a).

⁶ Electronic Frontier Foundation, “Who Has Your Back? Government Data Requests 2017,” Rainey Reitman, July 10, 2017, <https://www.eff.org/who-has-your-back-2017>.

⁷ The New York Times, “Secret F.B.I. Subpoenas Scoop Up Personal Data From Scores of Companies,” Jennifer Valentino-DeVries, September 20, 2019, <https://www.nytimes.com/2019/09/20/us/data-privacy-fbi.html>. Washington Post, “Secretive FBI demands for information go far beyond tech companies, new documents reveal,” Craig Timberg and Devlin Barrett, September 20, 2019, <https://www.washingtonpost.com/technology/2019/09/20/secretive-fbi-demands-information-go-far-beyond-tech-companies-new-documents-reveal/>.

⁸ USA FREEDOM Act of 2015, H.R. 2048, 114th Cong., § 502(f).

⁹ Wired, “Yahoo Publishes National Security Letters After FBI Drops Gag Orders,” Kim Zetter, June 1, 2016, <https://www.wired.com/2016/06/yahoo-publishes-national-security-letters-fbi-drops-gag-orders/>; Richard Salgado, Sharing National Security Letters with the public (Dec. 13, 2016), <https://www.blog.google/outreach-initiatives/public-policy/sharing-national-security-letters-public/>; Cloudflare, “Cloudflare’s Transparency Report for Second Half 2016 and an Additional Disclosure for 2013,” Kenneth R. Carter, January 10, 2017, <https://blog.cloudflare.com/cloudflares-transparency-report-for-second-half-2016-and-an-additional-disclosure-for-2013-2/>; Electronic Frontier Foundation, “Who Has Your Back? Government Data Requests 2017,” Rainey Reitman, July 10, 2017, <https://www.eff.org/who-has-your-back-2017>.

¹⁰ The New York Times, “Termination Letters,” Jennifer Valentino-DeVries, September 17, 2019, <https://www.documentcloud.org/public/search/projectid:45842-Termination-Letters>.

1. For what reason do you not report statistics about NSLs, although you are legally allowed to do so and it is considered a best practice?¹¹
 - a. Please provide any documentation of deliberations and communications regarding your company's chosen level of transparency about NSLs.
2. For each semiannual period since 2013, please answer the following questions:
 - a. To the maximum extent allowed by law, e.g., as detailed in 50 U.S.C. § 1874, please describe the number of received NSLs and other categories of legal process received, and the number of customer selectors targeted under each category.
 - b. Did you receive any NSLs that were not accompanied by a nondisclosure order barring your company from notifying the user of the request?
 - c. How many nondisclosure orders were ultimately terminated by the receipt of a termination letter from the FBI?
3. What is the typical procedure that your company follows upon receiving requests for account data?
4. What kind of information is typically requested of your company? Please provide our offices with as many copies of NSLs (redacted to the extent required by law) as you are able.
5. Will you commit to reporting this information in the future to the maximum extent allowed by law?

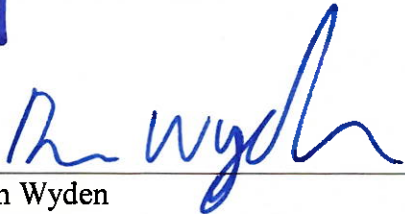
Sincerely,



Elizabeth Warren
United States Senator



Rand Paul
United States Senator



Ron Wyden
United States Senator

¹¹ Electronic Frontier Foundation, "Who Has Your Back? Government Data Requests 2017," Rainey Reitman, July 10, 2017, <https://www.eff.org/who-has-your-back-2017>.

United States Senate

WASHINGTON, DC 20510

December 12, 2019

Craig Boundy
Chief Executive Officer
Experian North America
475 Anton Blvd.
Costa Mesa, CA 92626

Dear Mr. Boundy:

We write with alarm about your company's failure to provide transparency into your receipt, handling, and reporting of consumer information through national security letters (NSLs) from the Federal Bureau of Investigation (FBI). NSLs are akin to administrative subpoenas that require the recipient to divulge information that the FBI deems relevant to national security investigations, including sensitive information on the company's consumers, including names, addresses, billing records, and even full credit reports. The FBI can send NSLs without gaining prior approval from a judge.^{1,2}

In September, the Electronic Frontier Foundation released a large set of documents gained via a Freedom of Information Act lawsuit indicating that credit reporting agencies such as yours have frequently been the recipients of NSLs, a fact which previously was not publicly known.³

As one of the three credit reporting agencies in the US, your company collects and sells credit information on vast numbers of Americans. Experian boasts that it "maintains credit information on approximately 220+ million U.S. consumers and 40 million active U.S. businesses" and "maintains demographic information on approximately 300 million consumers in 126 million households across the U.S."⁴ Because your company holds so much potentially sensitive data on so many Americans and collects this information without obtaining consent from these individuals, you have a responsibility to protect individuals' data and be transparent about how or when you disclose it. Unfortunately, your company has not provided information to policymakers or the public about the type or the number of disclosures that you have made to the FBI.

¹ New York Times, "Secret F.B.I. Subpoenas Scoop Up Personal Data From Scores of Companies," Jennifer Valentino-DeVries, September 20, 2019. <https://www.nytimes.com/2019/09/20/us/data-privacy-fbi.html>.

² Congressional Research Service, "National Security Letters in Foreign Intelligence Investigations: Legal Background," Charles Doyle, July 30, 2015, <https://fas.org/sgp/crs/intel/RL33320.pdf>.

³ New York Times, "Secret F.B.I. Subpoenas Scoop Up Personal Data From Scores of Companies," Jennifer Valentino-DeVries, September 20, 2019. <https://www.nytimes.com/2019/09/20/us/data-privacy-fbi.html>.

⁴ Experian, "Experian's Corporate Fact Sheet," accessed December 9, 2019, <http://www.experian.com/corporate/experian-corporate-factsheet.html>.

The USA FREEDOM Act was intended, in part, to increase the level of transparency around NSLs. Section 603 of the Act specifically permits entities that receive NSLs to report aggregated information about them, including the number of NSLs received.⁵ Dozens of technology and telecommunication companies publish reports of statistics about their receipt of NSLs.⁶ But Experian maintains no such publicly available information and has not provided information about NSL receipt when asked by reporters.⁷

NSLs are typically accompanied by nondisclosure orders that prevent recipients from disclosing that they have received the letter. Section 502(f) of the Act requires the government to periodically review these nondisclosure orders and determine whether the orders can be terminated. It also requires the government to send notification, in the form of a so-called “termination letter,” to NSL recipients if and when the nondisclosure order is terminated. This allows the recipient to speak.⁸ Some companies routinely publish NSLs upon their receipt of termination letters.⁹

The records disclosed by the Electronic Frontier Foundation show that Experian has received dozens of termination letters from the FBI that terminate NSL nondisclosure orders.¹⁰ Yet, although it is no longer barred from discussing those NSLs, your company has not published anything about them. Such publications give the public a sense of the content that companies share with the FBI. American consumers deserve to know what happens to the data that your company collects, which can encompass all of the major financial relationships that a consumer might have over the course of their lifetime.

To provide clarity about how your company provides sensitive consumer financial data to the government, we ask that you answer the following questions no later than December 27, 2019.

⁵ USA FREEDOM Act of 2015, H.R. 2048, 114th Cong., § 603(a).

⁶ Electronic Frontier Foundation, “Who Has Your Back? Government Data Requests 2017,” Rainey Reitman, July 10, 2017, <https://www.eff.org/who-has-your-back-2017>.

⁷ The New York Times, “Secret F.B.I. Subpoenas Scoop Up Personal Data From Scores of Companies,” Jennifer Valentino-DeVries, September 20, 2019, <https://www.nytimes.com/2019/09/20/us/data-privacy-fbi.html>. Washington Post, “Secretive FBI demands for information go far beyond tech companies, new documents reveal,” Craig Timberg and Devlin Barrett, September 20, 2019, <https://www.washingtonpost.com/technology/2019/09/20/secretive-fbi-demands-information-go-far-beyond-tech-companies-new-documents-reveal/>.


⁸ USA FREEDOM Act of 2015, H.R. 2048, 114th Cong., § 502(f).

⁹ Wired, “Yahoo Publishes National Security Letters After FBI Drops Gag Orders,” Kim Zetter, June 1, 2016, <https://www.wired.com/2016/06/yahoo-publishes-national-security-letters-fbi-drops-gag-orders/>; Richard Salgado, Sharing National Security Letters with the public (Dec. 13, 2016), <https://www.blog.google/outreach-initiatives/public-policy/sharing-national-security-letters-public/>; Cloudflare, “Cloudflare’s Transparency Report for Second Half 2016 and an Additional Disclosure for 2013,” Kenneth R. Carter, January 10, 2017, <https://blog.cloudflare.com/cloudflares-transparency-report-for-second-half-2016-and-an-additional-disclosure-for-2013-2/>; Electronic Frontier Foundation, “Who Has Your Back? Government Data Requests 2017,” Rainey Reitman, July 10, 2017, <https://www.eff.org/who-has-your-back-2017>.

¹⁰ The New York Times, “Termination Letters,” Jennifer Valentino-DeVries, September 17, 2019, <https://www.documentcloud.org/public/search/projectid:45842-Termination-Letters>.

1. For what reason do you not report statistics about NSLs, although you are legally allowed to do so and it is considered a best practice?¹¹
 - a. Please provide any documentation of deliberations and communications regarding your company's chosen level of transparency about NSLs.
2. For each semiannual period since 2013, please answer the following questions:
 - a. To the maximum extent allowed by law, e.g., as detailed in 50 U.S.C. § 1874, please describe the number of received NSLs and other categories of legal process received, and the number of customer selectors targeted under each category.
 - b. Did you receive any NSLs that were not accompanied by a nondisclosure order barring your company from notifying the user of the request?
 - c. How many nondisclosure orders were ultimately terminated by the receipt of a termination letter from the FBI?
3. What is the typical procedure that your company follows upon receiving requests for account data?
4. What kind of information is typically requested of your company? Please provide our offices with as many copies of NSLs (redacted to the extent required by law) as you are able.
5. Will you commit to reporting this information in the future to the maximum extent allowed by law?

Sincerely,


Elizabeth Warren
United States Senator


Rand Paul
United States Senator


Ron Wyden
United States Senator

¹¹ Electronic Frontier Foundation, "Who Has Your Back? Government Data Requests 2017," Rainey Reitman, July 10, 2017, <https://www.eff.org/who-has-your-back-2017>.

United States Senate

WASHINGTON, DC 20510

December 12, 2019

Christopher A. Cartwright
President and Chief Executive Officer
TransUnion
555 West Adams St
Chicago, IL 60661

Dear Mr. Cartwright:

We write with alarm about your company's failure to provide transparency into your receipt, handling, and reporting of consumer information through national security letters (NSLs) from the Federal Bureau of Investigation (FBI). NSLs are akin to administrative subpoenas that require the recipient to divulge information that the FBI deems relevant to national security investigations, including sensitive information on the company's consumers, including names, addresses, billing records, and even full credit reports. The FBI can send NSLs without gaining prior approval from a judge.^{1,2}

In September, the Electronic Frontier Foundation released a large set of documents gained via a Freedom of Information Act lawsuit indicating that credit reporting agencies such as yours have frequently been the recipients of NSLs, a fact which previously was not publicly known.³

As one of the three credit reporting agencies in the US, your company collects and sells credit information on vast numbers of Americans. TransUnion boasts of possessing "more than 200 million files profiling nearly every credit-active consumer in the United States."⁴ Because your company holds so much potentially sensitive data on so many Americans and collects this information without obtaining consent from these individuals, you have a responsibility to protect individuals' data and be transparent about how or when you disclose it. Unfortunately, your company has not provided information to policymakers or the public about the type or the number of disclosures that you have made to the FBI.

The USA FREEDOM Act was intended, in part, to increase the level of transparency around NSLs. Section 603 of the Act specifically permits entities that receive NSLs to report aggregated

¹ New York Times, "Secret F.B.I. Subpoenas Scoop Up Personal Data From Scores of Companies," Jennifer Valentino-DeVries, September 20, 2019. <https://www.nytimes.com/2019/09/20/us/data-privacy-fbi.html>.

² Congressional Research Service, "National Security Letters in Foreign Intelligence Investigations: Legal Background," Charles Doyle, July 30, 2015, <https://fas.org/sgp/crs/intel/RL33320.pdf>.

³ New York Times, "Secret F.B.I. Subpoenas Scoop Up Personal Data From Scores of Companies," Jennifer Valentino-DeVries, September 20, 2019. <https://www.nytimes.com/2019/09/20/us/data-privacy-fbi.html>.

⁴ TransUnion, "Customer Credit Reporting," accessed December 9, 2019, <https://www.transunion.com/solution/customer-credit-check>.

information about them, including the number of NSLs received.⁵ Dozens of technology and telecommunication companies publish reports of statistics about their receipt of NSLs.⁶ But TransUnion maintains no such publicly available information and has not provided information about NSL receipt when asked by reporters.⁷

NSLs are typically accompanied by nondisclosure orders that prevent recipients from disclosing that they have received the letter. Section 502(f) of the Act requires the government to periodically review these nondisclosure orders and determine whether the orders can be terminated. It also requires the government to send notification, in the form of a so-called “termination letter,” to NSL recipients if and when the nondisclosure order is terminated. This allows the recipient to speak.⁸ Some companies routinely publish NSLs upon their receipt of termination letters.⁹

The records disclosed by the Electronic Frontier Foundation show that TransUnion has received dozens of termination letters from the FBI that terminate NSL nondisclosure orders.¹⁰ Yet, although it is no longer barred from discussing those NSLs, your company has not published anything about them. Such publications give the public a sense of the content that companies share with the FBI. American consumers deserve to know what happens to the data that your company collects, which can encompass all of the major financial relationships that a consumer might have over the course of their lifetime.

To provide clarity about how your company provides sensitive consumer financial data to the government, we ask that you answer the following questions no later than December 27, 2019.

⁵ USA FREEDOM Act of 2015, H.R. 2048, 114th Cong., § 603(a).

⁶ Electronic Frontier Foundation, “Who Has Your Back? Government Data Requests 2017,” Rainey Reitman, July 10, 2017, <https://www.eff.org/who-has-your-back-2017>.

⁷ The New York Times, “Secret F.B.I. Subpoenas Scoop Up Personal Data From Scores of Companies,” Jennifer Valentino-DeVries, September 20, 2019, <https://www.nytimes.com/2019/09/20/us/data-privacy-fbi.html>. Washington Post, “Secretive FBI demands for information go far beyond tech companies, new documents reveal,” Craig Timberg and Devlin Barrett, September 20, 2019, <https://www.washingtonpost.com/technology/2019/09/20/secretive-fbi-demands-information-go-far-beyond-tech-companies-new-documents-reveal/>.


⁸ USA FREEDOM Act of 2015, H.R. 2048, 114th Cong., § 502(f).

⁹ Wired, “Yahoo Publishes National Security Letters After FBI Drops Gag Orders,” Kim Zetter, June 1, 2016, <https://www.wired.com/2016/06/yahoo-publishes-national-security-letters-fbi-drops-gag-orders/>; Richard Salgado, Sharing National Security Letters with the public (Dec. 13, 2016), <https://www.blog.google/outreach-initiatives/public-policy/sharing-national-security-letters-public/>; Cloudflare, “Cloudflare’s Transparency Report for Second Half 2016 and an Additional Disclosure for 2013,” Kenneth R. Carter, January 10, 2017, <https://blog.cloudflare.com/cloudflares-transparency-report-for-second-half-2016-and-an-additional-disclosure-for-2013-2/>; Electronic Frontier Foundation, “Who Has Your Back? Government Data Requests 2017,” Rainey Reitman, July 10, 2017, <https://www.eff.org/who-has-your-back-2017>.


¹⁰ The New York Times, “Termination Letters,” Jennifer Valentino-DeVries, September 17, 2019, <https://www.documentcloud.org/public/search/projectid:45842-Termination-Letters>.

1. For what reason do you not report statistics about NSLs, although you are legally allowed to do so and it is considered a best practice?¹¹
 - a. Please provide any documentation of deliberations and communications regarding your company's chosen level of transparency about NSLs.
2. For each semiannual period since 2013, please answer the following questions:
 - a. To the maximum extent allowed by law, e.g., as detailed in 50 U.S.C. § 1874, please describe the number of received NSLs and other categories of legal process received, and the number of customer selectors targeted under each category.
 - b. Did you receive any NSLs that were not accompanied by a nondisclosure order barring your company from notifying the user of the request?
 - c. How many nondisclosure orders were ultimately terminated by the receipt of a termination letter from the FBI?
3. What is the typical procedure that your company follows upon receiving requests for account data?
4. What kind of information is typically requested of your company? Please provide our offices with as many copies of NSLs (redacted to the extent required by law) as you are able.
5. Will you commit to reporting this information in the future to the maximum extent allowed by law?

Sincerely,


Elizabeth Warren
United States Senator


Rand Paul
United States Senator


Ron Wyden
United States Senator

¹¹ Electronic Frontier Foundation, "Who Has Your Back? Government Data Requests 2017," Rainey Reitman, July 10, 2017, <https://www.eff.org/who-has-your-back-2017>.