September 27, 2022

The Honorable Lina Khan
Chair
Federal Trade Commission
600 Pennsylvania Avenue, NW
Washington DC 20580

Dear Chair Khan,

We write to express serious concern regarding the anti-competitive and anti-consumer practices of the nation's largest providers of verification services for income and employment backgrounds, as well as the near-ubiquitous collection and sale of payroll data, including personal identifiable information. We respectfully request that the Federal Trade Commission (FTC) undertake a sector-wide investigation of these practices.

As you commented in April 2022, "The general lack of legal limits on what types of information can be monetized has yielded a booming economy built around the buying and selling of this data," which "seems to incentivize endless tracking and vacuuming up of users' data."[1] An FTC blog from July 2022 also drew attention to "the often shadowy ad tech and data broker ecosystem where companies have a profit motive to share data at an unprecedented scale and granularity."[2] The country's largest data brokers have propelled this trend, specifically in the case of worker payroll data.

Using their historically dominant positions in the credit reporting industry, companies like Equifax and Experian have collected hundreds of millions of payroll records on everyday American consumers, which they sell to lenders, landlords, debt collectors, and other customers as part of their workforce verification services. More recently, these same brokers have aimed to secure exclusive access to payroll data through partnerships with major HR software providers, effectively turning the market for payroll data into an oligopoly. In turn, this business model has created unique harms to consumer privacy, data security, choice, and financial security, and it has led to business practices that stifle innovation and competition.

---

[1] Lima, C. & Schaffer, A. (2022, April 12). Analysis | FTC chair Lina Khan calls for a paradigm shift on data privacy. The Washington Post. (link)
[2] Cohen, K. (2022, July 11). Location, health, and other sensitive information: FTC committed to fully enforcing the law against illegal use and sharing of highly sensitive data. Federal Trade Commission. (link)

For context, millions of US employers send their workers' income and employment data to large-scale data brokers.[3] In theory, employers save money by outsourcing the work of handling requests for employment and income verification from third parties, such as landlords, lenders, and potential employers. Rather than contacting an employer's human resources (HR) department to verify a worker's background, these third parties purchase employment and income data from brokers that collect and sell hundreds of billions of personal records.[4] This verification system has dominated the US workforce for decades, partly because for many years, there was no clear alternative to this process.

However, new technologies are emerging every day that provide workers with safer, more secure, and more empowering tools to manage both their personal data and the verification process. For example, Certree provides workers with personal, private vaults where only they can review their data and safely share that tamper-free information with specific third parties with guaranteed authenticity. Yet companies like ours face enormous obstacles competing in a market where major players use their overwhelming scale and ability to incentivize exclusivity arrangements to undercut competitors. Meanwhile, Americans are suffering under a verification system in which workers are treated like products, not consumers.

In this letter, we discuss how:

- Major data brokers use anti-competitive practices to weaken consumer power and extract premium pricing by securing exclusive access to payroll data.

- Brokers' employment verification services have dangerous ramifications for consumers due to an abundance of inaccurate data and a systemic lack of consent that makes consumers bystanders in their own careers and financial lives.

- The FTC should investigate these practices as potential violations of the FTC Act.

[3] Chmura, C. (2022, February 15). A data broker has millions of workers' paystubs; see if they have yours. NBC Bay Area. (link)
[4] Equifax Inc., (2022). 2021 Annual Report (link)

1. Major payroll data brokers use financial considerations, service bundling, and historically dominant market positions to secure exclusivity deals and stifle competition.

Payroll data has become a highly prized commodity for data brokers. Late last year, one market expert estimated the total addressable market for payroll connectivity and data software at roughly $10 billion.[5] Alongside this development, brokers like Equifax and Experian have substantially increased the amount of payroll data they collect and sell, expanded the partnerships that supply them with payroll data, and found ways to combine payroll data with other information sources to undercut competitors.

It is our understanding that these brokers even offer distinct financial incentives to employers to gain exclusive access to their workers' personal data. Our experience in this industry has yielded several conversations with salespeople, former executives, and other workers at these brokers' client companies, many of whom attest to "loyalty-rewards" that brokers offer to employers that consider ending their contracts and withholding their payroll data from these brokers. In some cases, we understand that brokers have offered to share the revenue derived from worker data with that worker's employer, often guaranteeing the employer a minimum amount of revenue. This system enables both the brokers and the employers to monetize a worker's most personal information, leading to the neglect of worker privacy, data security, and consumer choice.

A. Equifax

As early as 2017, it was reported that Equifax's The Work Number subsidiary, which houses Equifax's employment verification services, collected payroll data on 85% of the federal government workforce, 75% of Fortune 500 companies, and countless state governments, agencies, courts, colleges, and small businesses.[6] As of 2022, Equifax collects payroll data on more than half of the entire US workforce,[7] and the company claims to hold more than 250 billion personal records. [8]

---

[5] Pimentel, B. (2021, August 31). Payroll data is fintech's $10 billion 'holy grail'. Protocol. (link)
[6] Winston, J. (2017, November 8). Facebook and America's largest companies quietly give worker data to Equifax. Fast Company. (link)
[7] Chmura, C. (2022, May 6). Your Pay Stub is Probably in the Cloud; Silicon Valley Startup Recommends a 'Vault' Instead. NBC Bay Area. (link)
[8] Equifax 2021 Annual Report (link)

This immense scale is largely the product of partnerships, exclusivity deals, and acquisitions that inhibit competition. Intuit recently told the 1.4 million small businesses using its QuickBooks and Intuit Online Payroll Systems that their payroll information would be shared with Equifax.[9] In May, Equifax became the exclusive provider of income and employment verifications for Paycor, an HR software company that claims to support more than 2 million users.[10] On the Workforce Partners section of its website, Equifax states this new partnership means "Paycor has a secure integration connection to provide employee data each pay cycle…"[11] That same page lists more than 30 partners in HR software[12], including ADP (with more than 20 million users on its mobile platform alone)[13], Ceridian (5.1 million users),[14] and PrismHR (2 million users)[15], among others. Like Paycor, many of these partners agree to provide Equifax with direct access to the millions of payroll records they collect. Brokers like Equifax often buy payroll data without explicit consent from the payroll companies' customers, or from the employees of those corporate customers. Much of the time, these are exclusive arrangements.

All this adds to Equifax's persistent efforts to concentrate the market by acquiring verification services that may challenge the company's access to consumer data. In fiscal 2021 alone, Equifax made acquisitions worth almost $3 billion, including the purchase of employee screening and verification services HIREtech and i2Verify.[16]

The incentives to seal off sources of payroll data are clear. In its 2021 Annual Report, Equifax described its Workforce Solutions segment, which broadly captures employee screening and verification, as "our fastest growing, highest margin and most valuable business […] Workforce Solutions has grown from about 25% of our total revenue 3 years ago to over 40% in 2021 and will likely grow to over 50% of Equifax in the coming years."[17] Meanwhile, Equifax

---

[9] Krebs, B. (2021, July 1). Intuit to Share Payroll Data from 1.4M Small Businesses With Equifax. Krebs on Security. (link)
[10] Paycor. (2022, May 4). Equifax Workforce Solution and Paycor Launch An Integrated Partnership To Automate Income and Employment Verification. PR Newswire. (link)
[11] Equifax Inc. (n.d.). Workforce Solutions, Partner Network. (link)
[12] Ibid.
[13] ADP, LLC (2019, March 28). ADP Mobile App Surpasses 20 Million Registered Users as the Mobile-First Movement Arrives in the Workplace. PR Newswire. (link)
[14] Ceridian HCM Holding Inc. (2022, February 9). Ceridian Reports Fourth Quarter and Full Year 2021 Results. (link)
[15] PrismHR. (n.d.). About. (link)
[16] Equifax 2021 Annual Report (link)
[17] Equifax Inc. (2022). Notice of 2022 Annual Meeting and Proxy Statement. (link)

increased the price of its employment verification services by 31% between August 2020 and March 2022, forcing consumers applying for loans, mortgages, and apartment rentals to pay higher fees as part of their application process.[18]

B. Experian

Similar to Equifax, Experian has made sizable acquisitions in the employment verification space. In fiscal 2020 alone, the company spent more than $580 million in cash on acquisitions, including payroll data competitors like Tax Credit Co, Corporate Cost Control, and Emptech.[19] On its own, the acquisition of Tax Credit Co required "a cash consideration of US$252m and contingent consideration of up to US$110m, determined by revenue and profit performance."[20] All this, combined with Experian's data on over 300 million consumers,[21] culminated in the launch of Experian's own employment verification service in May 2021.[22]

Importantly, in addition to acquisitions and partnerships, Experian is also known to use its dominant market position to cut out competition by bundling its services or offering revenue-sharing to provide a lower overall cost to clients that small-scale competitors cannot match. Again, our experience in this industry has yielded several conversations with executives and industry experts who have described this practice.

2. Between deceptive messaging around data uses, flawed data, and a systemic lack of well-informed consent, major brokers threaten consumer privacy and choice.

In a January 2022 statement, Rohit Chopra, the Director of the Consumer Financial Protection Bureau (CFPB), argued that "America's credit reporting oligopoly has little incentive to treat consumers fairly."[23] That same statement highlighted how "consumers submitted more than 700,000 complaints to the CFPB regarding the nation's largest data brokers from January 2020 through

[18] Wells, D. (2022, March 21). How The Work Number Cheats American Consumers. RealClearPolicy. (link)
[19] Experian plc. (2021, May 19). Full-year financial report. Release. (link)
[20] Experian plc. (2022). Experian Annual Report 2022. (link)
[21] Experian plc. (2018). ConsumerView. (link)
[22] Experian plc. (2021, May 24). Experian Announces New Employer Services Business and Real-time Income and Employment Verification Solution. businesswire. (link)
[23] Consumer Financial Protection Bureau. (2022, January 5). CFPB Releases Report Detailing Consumer Complaint Response Deficiencies of the Big Three Credit Bureaus. Release. (link)

September 2021, which represented more than 50% of all complaints received by the agency for that period."

A. Deceptive Practices

The nation's largest credit agencies have a history of misleading everyday consumers. In 2005, for instance, Experian reached a settlement with the FTC after it was charged with deceiving consumers by offering a "free" credit report through a system that charged $79.95 if customers did not cancel the service within 30 days.[24] In another instance, major data brokers received CFPB fines totaling more than $25 million in 2017 for "deceiving consumers in marketing credit scores." [25] [26]

When it comes to the broad, unchecked uses of worker payroll data, Equifax has recently been telling one story to the public and an entirely different story to its investors. Just last month, Duke Senior Fellow Justin Sherman published an analysis that addressed Equifax Senior Vice President Joe Muchnick's March 2022 interview with the Washington Post, in which he is quoted saying that the payroll data shared with The Work Number "is not passed on to other parts of Equifax, and is stored completely separately."[27] But as Sherman points out, Equifax boasts in its 2021 Annual Report that it's data fabric "unifies more than 100 data silos into a single platform," and the first dataset listed is The Work Number Database, which includes "136 million active payroll records, over 500 million historic records, from more than 2 million different US employers."[28] This integration is part of Equifax's campaign to build a "360 degree consumer view" by providing its corporate customers with data on a person's income, employment, education, credit, bank balances, criminal history, and more.[29]

B. Flawed Data

When brokers collect and sell inaccurate data, it poses a huge threat to workers' well-being. In 2016 and 2017, for example, job seekers filed lawsuits against

[24] Federal Trade Commission. (2005, August 16). Marketer of Free Credit Reports Settles FTC Charges. (link)
[25] Consumer Financial Protection Bureau. (2017, March 23). CFPB Fines Experian $3 Million for Deceiving Consumers in Marketing Credit Scores. Release. (link)
[26] Consumer Financial Protection Bureau. (2017, January 3). CFPB Orders TransUnion and Equifax to Pay for Deceiving Consumers in Marketing Credit Scores and Credit Products. Release. (link)
[27] Sherman, J. (2022, August 24). Examining data broker Equifax's relationships with millions of employers. Duke University's Sanford School of Public Policy. (link)
[28] Equifax 2021 Annual Report (link)
[29] Equifax Decision 360. (2010, May 10). Decision 360. (link)

Starbucks claiming they were denied jobs at the company due to flawed data in their background checks.[30] Starbucks denied the charges but reached a class-action settlement with roughly 8,000 job seekers, with the largest settlements going to people who "were unable to get any job or a similar job for at least 30 days."[31] And this is just one example of the types of lawsuits under the Fair Credit Reporting Act (FCRA) that have surged over the past ten years. Since 2011, the number of FCRA-related lawsuits has nearly tripled, reaching more than 5,400 lawsuits in 2021 alone.[32]

In the broker-centered system for verifying backgrounds, this type of large-scale data error is largely unavoidable. CNBC reports that major data brokers must now update more than one billion pieces of data every month.[33] At this enormous scale, it is perhaps unsurprising that one FTC study of consumers, lenders, and brokers found that 21% of respondents had successfully disputed at least one data error in their reports.[34] As a result of this faulty data, workers are denied opportunities for jobs, loans, apartments, and more every year.

And because the broker-centered model of employment verification completely bypasses the workers whose data is being verified, many workers never know that flawed data is the cause of these missed opportunities.

Moreover, even when consumers find errors in the data collected by major brokers, it can be nearly impossible to resolve those errors. According to a recent CFPB report, "In 2021, the nation's largest data brokers together reported relief in response to less than 2% of covered complaints."[35]

C. Abuse of Consent and Inability to Opt Out

Despite the breadth of the broker-centered system for employment verification, many workers are unaware that their employers share their private salary data with major brokers. Earlier this year, the Washington Post outlined that many

---

[30] Thibodeau, P. & Holland, M. (2021, December 20). Employee background check errors harm thousands of workers. TechTarget. (link)
[31] Ibid.
[32] True Hire.com (2022, May 12). FCRA lawsuits reach new record in 2021 after decade of steady increase. (link)
[33] Klein, A. (2017, September 27). The real problem with credit reports is the astounding number of errors. CNBC. (link)
[34] Federal Trade Commission. (2015, January). Report to Congress Under Section 319 of the Fair and Accurate Credit Transactions Act of 2003. (link)
[35] Consumer Financial Protection Bureau. (2022, January 5). CFPB Releases Report Detailing Consumer Complaint Response Deficiencies.

workers at Google were unaware their employer regularly shared their payroll data with Equifax's The Work Number service, with Google workers identifying this practice as one of the top concerns they wanted executives to address. [36] Around the same time, many Apple workers learned from national headlines that their employer recorded former workers as "associates" regardless of their actual titles.[37] Once again, some workers were surprised to learn this inaccurate data was regularly shared with InVerify, a verification service owned by Equifax.

Payroll data is distinct in the discussion of digital privacy as workers have virtually no practical ability to opt out of this system. Equifax alone collects payroll data from most US employers, and other major brokers collect data on a sizable share of the remaining workforce. Therefore, job seekers face a steep uphill climb to find a viable employer that is also willing to protect their digital privacy. As Justin Sherman argues in the same analysis discussed above, consumers "are forced to have their data collected, monetized, and shared in order to access employment opportunities."[38]

Moreover, since the consent form for income verification is normally presented by a lender during the application process for a loan or mortgage, it is highly unlikely that most workers are presented with the full scope of how brokers like Equifax will use their data once the consent is granted. As noted above, Equifax is creating a "360 degree" view of consumers, and it is difficult to see how tens of millions of workers gave well-informed consent for their payroll data to be part of this venture.

Sherman concludes his analysis of this broker-centered verification system saying that "a market […] in which workers are essentially powerless to the sharing and monetization of their own information is not one in which that consent is full, informed, and freely given."[39]

Additionally, Equifax and Experian do not always directly verify the consent behind the data they sell. Rather, they often rely on intermediary data buyers to obtain that consent, and major brokers take it for granted that this consent is well-informed and authentic.

---

[36] Albergotti, R. & De Vynck, G. (2022, March 23). Tech workers are upset their companies are sharing payroll data with Equifax. Here's what's going on. The Washington Post. (link)
[37] Albergotti, R. (2022, February 10). Every employee who leaves Apple becomes an 'associate'. The Washington Post. (link)
[38] Sherman, J. (2022, August 24). Examining Equifax's relationships. Duke. (link)
[39] Ibid.

This systemic lack of consent could represent a violation of Section 5 of the FTC Act.

D. Pattern of Large-Scale Data Breaches

A lack of meaningful consent from workers, combined with clear incentives for brokers to collect and share as much data as possible, is especially dangerous because the nation's largest brokers have a history of exposing the highly sensitive data they collect. In 2017, for example, Equifax announced a data breach that exposed the personal information of 147 million people.[40] An FTC investigation into this breach later noted Equifax's "failure to take reasonable steps to secure its network."[41] That same year, it was reported that hackers had begun using Americans' dates of birth and Social Security Numbers, which had been exposed during the large-scale data breach, in order to change workers' PIN numbers and steal their W-2s using Equifax's Work Number subsidiary.[42] This security failure led to numerous independent breaches of worker data for employers such as Allegis, Northrop Grumman, Erickson Living, Saint-Gobain Group, and The University of Louisville, among others. [43]

Experian has also struggled with data security. Just last month, Krebs on Security reported that Experian now faces a class-action lawsuit in the California Central District Court after the public learned that Experian "did little to prevent identity thieves from hijacking consumer accounts […] simply by signing up for new accounts using the victim's personal information and a different email address."[44] In 2021, Experian API exposed the credit scores of most Americans. [45] In 2020, close to 800,000 businesses' private data was breached.[46] And in 2015, a breach at Experian exposed the Social Security numbers of roughly 15 million consumers.[47]

---

[40] Siegel Bernard, T. (2020, January 22). Equifax Breach Affected 147 Million, but Most Sit Out Settlement. The New York Times. (link)
[41] Federal Trade Commission. (2019, July 22). Equifax to Pay $575 Million as Part of Settlement with FTC, CFPB, and States Related to 2017 Data Breach. Release. (link)
[42] Krebs, B. (2017, May 18). Fraudsters Exploited Lax Security at Equifax's TALX Payroll Division (link)
[43] Ibid.
[44] Krebs, B. (2022, August 5). Class Action Targets Experian Over Account Security. Krebs on Security. (link)
[45] Krebs, B. (2021, April 28). Experian API Exposed Credit Scores of Most Americans. Krebs on Security. (link)
[46] Reuters Staff. (2020, August 19). S.African fraudster tricks credit bureau Experian into handing over data. (link)
[47] Krebs, B. (2015, October 2). Experian Breach Affects 15 Million Consumers. Krebs on Security. (link)

With so much sensitive data held by just a few data brokers, it is perhaps unavoidable that these brokers would be perennial targets for both large-scale and amateur hackers. In Equifax's 2021 Security Annual Report, the company even admits that it receives roughly 35 million cyber threats every single day.[48]

And with massive data breaches that expose consumers' Social Security numbers, dates of birth, and other personal details, brokers are also arming fraudsters with all the information they need to hack consumer accounts.[49]

Breaches like these have powerful and permanent consequences for individuals whose data is stolen and abused. And in this broker-centered market, workers are not consumers who can withhold spending to spur better security practices. Additionally, workers are not suppliers who can withhold their data. Rather, workers are treated as commodities with no influence over the system that buys and sells their personal data.

Unprecedented market practices and broad uses of personal payroll data require investigation by the FTC.

These practices could violate the FTC Act. The Commission should investigate Equifax and Experian and their respective employment verification services, market practices, and methods for collecting and selling payroll data. Specifically, the Commission should seek answers from these brokers to the following questions:

- Do you pay (or provide consideration to) employers that use your employment verification services in order to access their payroll data? If you do, are those relationships with employers exclusive?

- Has your company ever bundled verification services with any other services in order to reduce competition or win business from competitors? If so, did the customer have the option not to bundle their services through your company?

- Has your company ever offered a financial incentive (or rebate) to a customer that was considering ending, or had already ended, their relationship with your employment verification service?

[48] Equifax Inc. (2022). 2021 Security Annual Report. (link)
[49] Krebs, B. (2017, October 8). Equifax Breach Fallout: Your Salary History. Krebs on Security. (link)

- Have you ever proactively influenced an employer to have them add financial reward or service bundling in its pending RFP?

- When your company collects or receives payroll data, is that data used for your company's other business segments or any other purpose? Is that data aggregated, referenced, or used for any other business purposes or products?

- What processes does your company employ to ensure the income and employment data you sell is accurate?

- When an employer contracts with your employment verification services, are there any limits on how your company can use payroll records once the worker concerned has given consent?

- What steps do you take to ensure workers fully consent to all the potential and actual uses of their payroll data by your company?

- What steps do you take to ensure worker consent is authentic in order to prevent identity fraud and theft?

As you noted earlier this year, "businesses' access to and control over such vast troves of granular data on individuals can give those firms enormous power to predict, influence, and control human behavior. In other words, what's at stake with these business practices is not just one's subjective preference for privacy, but—over the long term—one's freedom, dignity, and equal participation in our economy and society."[50] We wholeheartedly agree, and we thank you for your attention to this important matter.

Respectfully Submitted,

Pavan Kochar
Chief Executive Officer
Certree

[50] Khan, L. (2022, April 11). Remarks of Chair Lina M. Khan As Prepared for Delivery IAPP Global Privacy Summit 2022 Washington, D.C. (link)

Cc:

Commissioner Alvaro Bedoya
Federal Trade Commission

Commissioner Noah Phillips
Federal Trade Commission

Commissioner Rebecca Slaughter
Federal Trade Commission

Commissioner Christine Wilson
Federal Trade Commission

Secretary April Tabor
Federal Trade Commission

Samuel Levine, Director, Bureau of Consumer Protection
Federal Trade Commission

Holly Vedova, Director, Bureau of Competition
Federal Trade Commission