UNITED STATES DISTRICT COURT

NORTHERN DISTRICT OF TEXAS

ERIC L. ELLIS, Plaintiff, vs. CARGILL MEAT SOLUTIONS, AND ULTIMATE KRONOS GROUP (UKG) Defendants	Case No.: 4-22CV-864-Y

PLAINTIFF'S ORIGINAL COMPLAINT

PARTIES

Plaintiff Eric L. Ellis is a male adult of sound mind and a employee of Cargill Meat Solutions whom is a resident of 8539 Melissa Dr Fort Worth, Texas 76108.

Defendant Cargill Meat Solutions is a business in the city of Fort Worth at address; 3709 E 1st St, Fort Worth, TX 76111. At all relevant times in this lawsuit, Cargill Meat Solutions acted as an employer of the Plaintiff, Eric Ellis.

Defendant Cargill Meat Solutions may be served by service upon its registered agent, UNITED AGENT GROUP INC.

5444 Westheimer #1000

Houston, TX 77056 USA, or by any other method allowed by law.

Defendant Ultimate Kronos Group (UKG) may be served by service upon its registered agent,

C T Corporation System

1999 Bryan St., Ste. 900

Dallas, TX 75201-3136 USA, or by any other method allowed by law.

JURISDICTION AND VENUE

The Court has subject-matter jurisdiction under 28 U.S.C. § 1331 and 28 U.S.C. § 1343.

Venue is proper because a substantial part of the events giving rise to the claims occurred in this judicial district. See 28 U.S.C. § 1391(b)(2).

This Court is empowered to issue a declaratory judgment and further relief pursuant to 28 U.S.C. § 2202.

This Court has also has original subject matter jurisdiction pursuant to 28 U.S.C. § 1331 because this action involves a federal question under the FLSA. 29 U.S.C. § 216(b).

COVERAGE UNDER THE FLSA

At all relevant times, Cargill Meat Solutions was an employer of Eric Ellis within the meaning of Section 3(d) of the FLSA, 29 U.S.C. § 203(d).

At all relevant times, Cargill Meat Solutions was and is an employer of Eric Ellis within the meaning of Section 3(d) of the FLSA, 29 U.S.C. § 203(d).

Cargill Meat Solutions was and is part of an enterprise within the meaning of Section 3(r) of the FLSA, 29 U.S.C. § 203(r).

During at least the last three years, Cargill Meat Solutions has had gross annual sales in excess of $500,000.

Cargill Meat Solutions was and is part of an enterprise engaged in commerce or in the production of goods for commerce within the meaning of the FLSA, 29 U.S.C. § 203(s)(1).

Cargill Meat Solutions employs many workers, including Eric Ellis, who are engaged in commerce or in the production of goods for commerce and/or who handle, sell, or otherwise work on goods or materials that have been moved in or produced for commerce by any person.

The goods and materials handled, sold, or otherwise worked on by Ellis, and other Cargill Meat Solutions' employees and that have been moved in interstate commerce include, but are not limited to, ready to eat foods and their component parts.

STATEMENT OF FACTS

Cargill Meat Solutions manufactures and distributes luxury and commercial automobiles.

Many of Cargill Meat Solutions's employees are non-exempt hourly and salaried workers.

Since at least 2021, Cargill Meat Solutions has used timekeeping software and hardware operated and maintained by Kronos.

On or about December 11, 2021, Kronos was hacked with ransomware.

The Kronos hack interfered with the ability of its customers, including Cargill Meat Solutions, to use Kronos's software and hardware to track hours and pay employees.

Since the onset of the Kronos hack, Cargill Meat Solutions has not kept accurate track of the hours that Ellis have worked.

Instead, Cargill Meat Solutions has used various methods to estimate the number of hours Ellis and Similarly Situated Workers work in each pay period.

For example, Cargill Meat Solutions issued paychecks based on scheduled hours or estimated hours, or simply duplicated paychecks from pay periods prior to the Kronos hack.

This means that employees who were non-exempt and worked overtime were in many cases paid less than the hours they worked in the workweek, including overtime hours.

Even if certain overtime hours were paid, the pay rate would be less than the full overtime premium. Many employees were not even paid their non-overtime wages for hours worked before 40 in a workweek.

Ellis is one of the employees affected by this decision by Cargill Meat Solutions and the resulting pay practice.

Instead of paying Ellis for the hours he actually worked (including overtime hours), Cargill Meat Solutions simply paid based on estimates of time or pay, or based upon arbitrary considerations other than Ellis's actual hours worked and regular pay rates.

In some instances, Ellis was paid portions of the overtime he worked, but the overtime rate he was paid was not at least 1.5 times his regular rate of pay, including required adjustments for shift differentials and non-discretionary bonuses.

In properly calculating and paying overtime to a non-exempt employee, the only metrics that are needed are: (1) the number of hours worked in a day or week, and (2) the employee's regular rate, taking into account shift differentials, non-discretionary bonuses, and other factors allowed under the law.

Cargill Meat Solutions knows it has to pay proper overtime premiums to nonexempt hourly and salaried employees.

Cargill Meat Solutions knows this because, prior to the Kronos hack, it routinely paid these workers for all overtime hours at the proper overtime rates.

Cargill Meat Solutions could have instituted any number of methods to accurately track and timely pay its employees for all hours worked.

Instead of accurately tracking hours and paying employees their overtime, Cargill Meat Solutions decided to arbitrarily pay these employees, without regard to the overtime hours they worked or the regular rates at which they were supposed to be paid.

Even if it did pay any overtime to affected employees, Cargill Meat Solutions did not take into account shift differentials and non-discretionary bonuses, such that the overtime premium Cargill Meat Solutions did pay, if any, was not the full overtime premium owed under the law based on the employees' regular rate.

It was feasible for Cargill Meat Solutions to have its employees and managers report accurate hours so they could be paid the full and correct amounts of money they were owed for the work they did for the company. But it chose not to do that.

In other words, Cargill Meat Solutions pushed the effects of the Kronos hack onto the backs of its most economically vulnerable workers, making sure that it kept the money it owed to those employees in its own pockets, rather than take steps to make sure its employees were paid on time and in full for the work they did.

Eric Ellis is just one of the many Cargill Meat Solutions employees who had to shoulder the burden of this decision by Cargill Meat Solutions.

Ellis was a non-exempt hourly employee of Cargill Meat Solutions.

Ellis regularly worked over 40 hours per week for Cargill Meat Solutions.

Ellis's normal, pre-Kronos hack hours are reflected in Cargill Meat Solutions records.

Since the Kronos hack, Cargill Meat Solutions has not paid Ellis for his actual hours worked each week.

Since the hack took place, Cargill Meat Solutions has not been accurately recording the hours worked by Ellis and its other workers.

Even when Cargill Meat Solutions has issued payment to Ellis for any overtime, the overtime is not calculated based on Ellis's regular rates, as required by federal law.

Cargill Meat Solutions was aware of the overtime requirements of the FLSA.

Cargill Meat Solutions nonetheless failed to pay the full overtime premium owed to certain non-exempt hourly and salaried employees, such as Ellis.

Cargill Meat Solutions's failure to pay overtime to these non-exempt workers was, and is, a willful violation of the FLSA.

The full overtime wages owed to Ellis became "unpaid" when the work for Cargill Meat Solutions was done—that is, on Ellis's regular paydays. E.g., Martin v. United States, 117 Fed. Cl. 611, 618 (2014); Biggs v. Wilson, 1 F.3d 1537, 1540 (9th Cir.1993); Cook v. United States, 855 F.2d 848, 851 (Fed. Cir. 1988); Olson v. Superior Pontiac–GMC, Inc., 765 F.2d 1570, 1579 (11th Cir.1985), modified, 776 F.2d 265 (11th Cir.1985); Atlantic Co. v. Broughton, 146 F.2d 480, 482 (5th Cir.1944); Birbalas v. Cuneo Printing Indus., 140 F.2d 826, 828 (7th Cir.1944).

At the time Cargill Meat Solutions failed to pay Ellis in full for his overtime hours by his regular paydays, Cargill Meat Solutions became liable for all prejudgment interest, liquidated damages, penalties, and any other damages owed under federal and Texas law.

In other words, there is no distinction between late payment and nonpayment of wages under federal law. Biggs v. Wilson, 1 F.3d 1537, 1540 (9th Cir.1993).

Even if Cargill Meat Solutions made any untimely payment of unpaid wages due and owing to Ellis any alleged payment was not supervised by the Department of Labor or any court.

The untimely payment of overtime wages, in itself, does not resolve a claim for unpaid wages under the law. See, e.g., Seminiano v. Xyris Enterp., Inc., 602 Fed.Appx. 682, 683 (9th Cir. 2015); Lynn's Food Stores, Inc. v. United States, 679 F.2d 1350, 1352-54 (11th Cir. 1982).

Nor does the untimely payment of wages, if any, compensate workers for the damages they incurred due to Cargill Meat Solutions's acts and omissions resulting in the unpaid wages in the first place.

Plaintiff, Eric Ellis remains uncompensated for the wages and other damages owed by Cargill Meat Solutions under federal law.

Like many other companies across the United States, Cargill Meat Solution's timekeeping and payroll systems were affected by the hack of Kronos in 2021.

That hack led to problems in timekeeping and payroll throughout Cargill's organization.

As a result, Cargill's employees who were not exempt from overtime under federal law were not paid for all overtime hours worked or were not paid their proper overtime premium after the onset of the Kronos hack.

Eric Ellis is one such Cargill worker.

Cargill could have easily implemented a system to accurately record time and properly pay non-exempt hourly and salaried employees until issues related to the hack were resolved.

But it didn't. Instead, Cargill Meat Solutions used prior pay periods or reduced payroll estimates to avoid paying wages and proper overtime to these nonexempt hourly and salaried employees.

Cargill Meat Solutions pushed the cost of the Kronos hack onto the most economically vulnerable people in its workforce.

Cargill Meat Solutions made the economic burden of the Kronos hack fall on front-line workers—average Americans—who rely on the full and timely payment of their wages to make ends meet.

Cargill's failure to pay wages, including proper overtime, for all hours worked violates the Fair Labor Standards Act (FLSA), 29 U.S.C. § 201, et seq.

Eric Ellis brings this lawsuit to recover these unpaid overtime wages and other damages owed by Cargill Meat Solutions because in reality he was the victim of not just the Kronos hack, but Cargill's decision to make its own non-exempt employees workers bear the economic burden for the hack.

Plaintiff Eric Ellis allege the following against Cargill Meat Solutions and Ultimate Kronos Group, (collectively, "Defendants") based upon the investigation of public information and personal experiences during his employment with Cargill.

This case involves a matter of growing concern in modern culture, that of the security of personal data and information in an era of exponential technological expansion. Specifically, this lawsuit against Cargill Meat Solutions and Ultimate Kronos Group arising from its failure to safeguard the Personal Identifying Information ("PII") of Cargill's employees by allowing fraudsters unauthorized access into Kronos's workforce management systems, (the "Data Breach"), which compromised Cargill's employees' PII.

Kronos is one of the largest Workforce Management service providers in the United States. Due to its size and the nature of its business, Kronos stores what hackers would consider a "treasure-trove" of PII from Cargill employees.

Because of the extensive confidential information that Kronos stores, Ultimate Kronos Group maintains a privacy policy that makes specific representations to its customers and affiliates regarding its affirmative duty to protect its customers' PII. In its Privacy Policy, Kronos represents to its customers that "To prevent unauthorized access or disclosure, to maintain data accuracy, and to allow only the appropriate use of your PII, UKG utilizes physical, technical, and administrative controls and procedures to safeguard the information we collect."

"To protect the confidentiality, integrity, availability and resilience of your PII, we utilize a variety of physical and logical access controls, firewalls, intrusion detection/prevention systems, network and database monitoring, anti-virus, and backup systems. We use encrypted sessions when collecting or transferring sensitive data through our websites."

"We limit access to your PII and data to those persons who have a specific business purpose for maintaining and processing such information. Our employees who have been granted access to your PII are made aware of their responsibilities to protect the confidentiality, integrity, and availability of that information and have been provided training and instruction on how to do so."

Cargill's employees reasonably expected Cargill to maintain strict confidentiality of their PII in Cargill's possession. However, Cargill Meat Solutions, contrary to its promises and representations, failed to adequately protect its employees' PII simply by providing the sensitive information to a third-party service provider "UKG" or Ultimate Kronos Group.

On December 12, 2021, Kronos began notifying its customers that the KRONOS Private Cloud (KPC) had been attacked by ransomware.

As a result of Kronos failure to maintain adequate security measures, Cargill Meat Solutions employees' personal and private information has been compromised and remains vulnerable.

The "ransomware attack" on UKG's weakened security system was a successful attempt by a malicious third party to access Kronos customers' PII on a mass scale. The only reason a hacker would steal or access PII on a mass scale would be to use that information to commit future acts of cyber-fraud and identity theft. It is a virtual certainty that the hackers will engage in future acts of fraud or identity theft either directly, or indirectly by selling the Kronos customers' PII on the dark web to other malicious actors. Thus, Plaintiff, is at an exceptionally high risk of future acts of identity theft. Moreover, the ill-gotten PII could be combined with information stolen during other computer hacks and data breaches to create increasingly complex and convincing scams.

As a direct result and a necessary consequence of the "Data Breach/Ransomware attack", the Plaintiff have suffered an ascertainable loss in that he must undertake additional security measures, some at his own expense, to minimize the risk of future data breaches.

Moreover, as a direct result and a necessary consequence of the Data Breach, Cargill's employees have suffered an ascertainable loss in that they have incurred otherwise unnecessary out-of-pocket expenses and suffered opportunity loss due to the time they have been required to spend in attempts to mitigate the damages caused by the Data Breach.

Furthermore, Kronos essentially granted unauthorized third parties/hackers access to Plaintiff's PII without compensating him. The value of his PII, in part derived from its privacy, should be exclusively controlled by Cargill, which is precisely what the Plaintiff expected.

As a result of Cargill and Kronos's failure to maintain adequate security measures, Plaintiff Eric Ellis continues to suffer an ongoing and escalating accumulation of damages, as the Data Breach

has rendered him more susceptible to future data breaches, identity theft, loss of wages and other kinds of online fraud.

Identity thieves can also use the PII to harm the Plaintiff through embarrassment, blackmail, or harassment either in person or online, or to commit other types of fraud including fraudulently obtaining tax returns and refunds, and government benefits -- as Kronos understands to be the case in this "ransomware attack".

A Presidential identity theft report from 2007 states that: In addition to the losses that result when identity thieves fraudulently open accounts or misuse existing accounts, . . . individual victims often suffer indirect financial costs, including the costs incurred in both civil litigations initiated by creditors and in overcoming the many obstacles they face in obtaining or retaining credit. Victims of non-financial identity theft, for example, health-related or criminal record fraud, face other types of harm and frustration. In addition to out-of-pocket expenses that can reach thousands of dollars for the victims of new account identity theft, and the emotional toll identity theft can take, some victims have to spend what can be a considerable amount of time to repair the damage caused by the identity thieves. Victims of new account identity theft, for example, must correct fraudulent information in their credit reports and monitor their reports for future inaccuracies, close existing bank accounts, open new ones, and dispute charges with individual creditors.

To put identity theft into context, the 2013 Norton Report – based on one of the largest consumer cybercrime studies ever conducted – estimated that at that time, the global price tag of cybercrime was around $113 billion with the average cost per victim being $298 dollars.

The problems associated with identity theft are exacerbated by the fact that many identity thieves will wait years before attempting to use the personal information they obtain. Indeed, to protect themselves, Plaintiff will need to remain vigilant against unauthorized data use for years and decades to come. It is axiomatic that once stolen, PII can be used in a number of different and sinister ways. One of the most common methods of illicit use is that the information is offered for sale on the "Dark Web," which is a heavily encrypted part of the internet that makes it difficult for authorities to detect the location or owners of a particular website. Due to its concealed and sometimes disguised nature, coupled with the intentional use of special applications to maintain anonymity, the Dark Web is a haven for a plethora of illicit activity, including the trafficking of stolen personal information captured via data breaches or hacks. A 2018 study found that an individual's online identity is worth as much as approximately $1,170 on the Dark Web. Scammers also use PII to target victims through phishing scams. Phishing occurs when scammers, using PII they have illicitly obtained about their victims, send fraudulent emails, texts, or copycat websites to get victims to share additional valuable PII – such as account numbers, Social Security numbers, or login IDs and passwords.

Scammers use victims' information, including PII, to steal victims' money, identity, or both. Scammers also use phishing emails to get access to a victim's computer or network, and then install programs like ransomware that can lock a victim out of important files on their computer. According to one Federal Bureau of Investigation study, scammers collected more than $676 million in 2017 alone through two types of phishing scams: "Business Email Compromise" and "Email Account Compromise." As a result of Kronos and Cargill's failure to maintain adequate security measures, the Plaintiff's PII has been compromised and remains vulnerable. The Plaintiff has suffered an ascertainable loss in that he must now undertake additional security measures, most at his own expense, to minimize the risk of future data breaches.

The Plaintiff's ascertainable losses in undertaking additional security measures is consistent with Javelin Strategy & Research's 2017 compilation of consumer complaints to the FTC showing that the average out-of-pocket cost to consumers for identity theft was $429.00. And the out-of-pocket costs is not a one-time occurrence. Instead, credit monitoring and protection should go on for no less than five years following a breach of this kind. According to the 2017 Ponemon report, the Consumer Financial Protection Bureau report as of 1Q 2017 and the Bureau of Justice Statistics ("BJS") between 2010 and 2014, stolen PII data is re-used for up to five years after a breach. In 2015, the last BJS report, commissioned on 2014 FTC data, calculated the average potential direct loss for unmonitored high value consumers to be $1,349 and out-of-pocket costs – including soft costs for full-time equivalent hours of missed work (potential loss

of income) due to time spent resolving identity theft issues – to be $3,903, with the average time to resolve a known identity theft being greater than one month.

These BJS independent surveys indicate that over 35% of victims have unresolved, related identity theft issues for up to one year after a breach and multiple non-commissioned surveys have also shown a high repeat occurrence of identity theft victims who are re-victimized less than three years from the original incident.

The Data Breach and disclosure of Kronos's customers' PII has immediately, directly and substantially increased Plaintiff's risk of identity theft. Also, as a result of the Data Breach, Plaintiff have suffered nuisance and a loss of privacy and must now expend additional time and money mitigating the threat of identity theft, which would not be necessary but for the Data Breach.

Plaintiff worked and continue to work hours for Defendant Cargill Meat Solutions that are not recorded or for which Plaintiff are not compensated, despite Defendants having knowledge that such hours are worked. Accordingly, Plaintiff is underpaid for the hours actually worked, often resulting in hourly rates that fall well below the minimum wage rates and overtime rates required by law.

Defendants do not consistently provide accurate pay stubs or wage statements. When pay stubs are actually provided, the wage statements are inaccurate, incomplete, manipulated and most times do not represent hours the plaintiff actually worked.

At all times material to this Complaint, the work performed by Plaintiff, has been jointly managed and supervised by Cargill Meat Solutions and "UKG" Ultimate Kronos Group. Upon information and belief, Plaintiff is employed directly by Defendant Cargill and Defendant Kronos is a workforce management company contracted by Cargill. Defendant Cargill Meat Solutions began having its employees fill out time sheets shortly after the Kronos Data Breach. Defendant Kronos oversees the payroll processing for Plaintiff. As such, each Defendant is considered an employer under the FLSA in their individual capacity.

Defendant Cargill Meat Solutions is the entity that pays wages to Plaintiff, however, upon information and belief, Cargill does not always provide accurate wage statements to the Plaintiff. Defendants' conduct, as set forth herein, was willful and in bad faith, and has caused significant damages to Plaintiff.

Although Defendants permitted and/or required the plaintiff to work upwards of 50+ hours per work week, Defendants have denied them compensation for all hours worked. As a result, the Plaintiff hourly rates of pay often fell below what was agreed in the employment contract, and he did not receive overtime compensation some weeks where he worked overtime.

Plaintiff Eric Ellis regularly work or have worked in excess of forty hours during a work week.

Plaintiff was not paid for all hours worked in a work week and resulting in diluted hourly rates and unpaid overtime wages for hours worked in excess of 40 in a work week.

Defendants' fraudulently misrepresenting the hours worked by the Plaintiff, and therefore diluting his hourly rate per hour and failing to compensate him for all hours worked in excess of 40 in a work week, in violation of the FLSA, forms the basis of the wage violation.

Plaintiff was not and is not exempt from receiving minimum wage or overtime pay under the FLSA.

Defendants' failure to pay overtime compensation at the rate required by the FLSA results from generally applicable practices, and does not depend on the personal circumstances of the Plaintiff.

The Plaintiff, irrespective of his particular job requirements, is entitled to accurate wage for all hours worked up to forty in a work week and are entitled to overtime compensation at the rate of time and a half for hours worked in excess of forty during a work week.

Although the exact amount of damages may vary, the damages can't be easily calculated by a simple formula due to the loss of data from the Kronos Data Breach or "Ransomware Attack".

The claims of the Plaintiff arise from a common nucleus of facts. Liability is based on a systematic course of wrongful conduct by the Defendants that caused harm to the Plaintiff.

These issues are known to Defendants, are readily identifiable, and can be located through Defendants' records.

FIRST CAUSE OF ACTION

Fair Labor Standards Act – Overtime Violations

Plaintiff incorporate by reference the allegations set forth above.

The FLSA requires that covered employees receive compensation for all hours worked and overtime compensation not less than one and one-half times the regular rate of pay for all hours worked in excess of forty hours in a work week. 29 U.S.C. § 207(a)(1).

At all times material herein, Plaintiff is covered employees entitled to the rights, protections, and benefits provided under the FLSA. 29 U.S.C. §§ 203(e) and 207(a).

Defendants are covered employers required to comply with the FLSA's mandates.

Defendants violated the FLSA with respect to Plaintiff, by, inter alia, failing to compensate Plaintiff for all hours worked and, with respect to such hours, failing to pay the legally mandated overtime premium for such work, as well as failing to provide compensation that is unconditional, free, and clear of deductions and/or kickbacks as described herein. Defendants also violated the FLSA by failing to keep required, accurate records of all hours worked by Plaintiff. 29 U.S.C. § 211(c).

Plaintiff is a victim of uniform and company-wide compensation policies instituted individually and separately by each Defendant. These uniform policies, in violation of the FLSA, are applied to current and former non-exempt, hourly laborers working throughout the United States, including in the State of Texas.

Defendants required Plaintiff to perform work before they clock in, i.e., using the manual time clock sheets since the Kronos "Ransomware Attack". Defendants also require Plaintiff to incur uncompensated "waiting time" hours. Defendants also manipulate Plaintiff's time records to fraudulently misrepresent the actual number of hours worked, depriving Plaintiff of compensation for all overtime hours worked.

Defendants have not paid and continue to refuse to pay Plaintiff overtime for all hours worked beyond 40 in each work week.

Upon information and belief, Defendant Cargill Meat Solution's violative overtime practices occur in a similar fashion across its numerous job sites around the United States.

Upon information and belief, Defendant Cargill's violative overtime practices occur in a similar fashion across multiple job sites around the State of Texas.

Plaintiff is entitled to damages equal to the mandated pay, including minimum wage, straight time, and overtime premium pay within the three years preceding the filing of the complaint, plus periods of equitable tolling, because Defendants have acted willfully and knew or showed reckless disregard for whether the alleged conduct was prohibited by the FLSA.

Defendants, and each of them, have acted neither in good faith nor with reasonable grounds to believe that their actions and omissions were not a violation of the FLSA, and as a result thereof, Plaintiff is entitled to recover an award of liquidated damages in an amount equal to the amount of unpaid overtime pay and/or prejudgment interest at the applicable rate. 29 U.S.C. § 216(b).

Defendants, in their capacity as individual and joint employers, willfully violated and continue to willfully violate the FLSA, by having engaged and continuing to engage in conduct which demonstrates a willful and/or reckless disregard for the provisions of the FLSA. Plaintiff spoke with managers or officers of Cargill Meat Solutions to alert them of the wage violations. Defendants were therefore on notice of their FLSA obligations and did not correct the violative practices.

As a result of the aforesaid violations of the FLSA's provisions, pay, including minimum wage, straight time, and overtime compensation, has been unlawfully withheld by Defendants from Plaintiff. Accordingly, Defendants are jointly and severally liable for unpaid wages, together with an amount equal as liquidated damages, attorneys' fees, and costs of this action.

Defendants violate the FLSA with respect to Plaintiff, by, inter alia, failing to compensate Plaintiff for all hours worked and, with respect to such hours, as well as failing to provide compensation that is unconditional, free, and clear of deductions and/or kickbacks as described herein. Defendants also violate the FLSA by failing to keep required, accurate records of all hours worked by Plaintiff and other employees. 29 U.S.C. § 211(c).

Defendants, in their capacities as individual and joint employers, dilute Plaintiff's regular hourly rates of pay below the minimum wage by fabricating, underreporting or otherwise artificially reducing the total hours reported worked by Plaintiff.

As a result, Defendants improperly diluted Plaintiff's regular hourly rates of pay and have not compensated Plaintiff for all hours worked.

Defendants, individually and/or jointly, have not paid and continue to refuse to pay Plaintiff for all hours worked during each work week.

Defendants, individually and/or jointly, violated the FLSA minimum wage by not properly compensating Plaintiff for all hours worked in a work week, thereby diluting his regular hourly rate.

Defendants' wage violations were and are willful.

As a result of Defendants' joint violations of the FLSA, Plaintiff is entitled to recover unpaid wages dating three (3) years from the date of this filing of this Complaint, plus an additional equal amount in liquidated damages, reasonable attorneys' fees, and costs of this action. Wherefore, Plaintiff request relief as hereinafter provided. As a direct and proximate result of Defendants' actions, Plaintiff have been and continue to be damaged, suffering economic harm, lost earnings and benefits, and other damages.

Defendants are liable to Plaintiff for civil penalties, damages, compensatory damages, and other relief including but not limited to injunctive relief, and all costs and attorneys' fees incurred in this action.

Wherefore, Plaintiff request relief as hereinafter provided.

SECOND CAUSE OF ACTION

NEGLIGENCE

Plaintiff incorporate by reference the allegations contained in each and every paragraph of this Complaint.

Cargill required the Plaintiff and other employees to submit sensitive PII in order to work for Cargill Meat Solutions. Cargill stored and shared this sensitive and valuable PII with The Ultimate Kronos Group.

By collecting, storing, using, and profiting from this data, Kronos had a duty of care to Plaintiff to exercise reasonable care in obtaining, retaining, securing, safeguarding, deleting, and protecting this PII in Kronos's possession from being compromised, lost, stolen, accessed, and misused by unauthorized persons. More specifically, this duty included, among other things:

(a) designing, maintaining, and testing Kronos's security systems and data storage architecture to ensure that Plaintiff's PII was adequately secured and protected;

(b) implementing processes that would detect an unauthorized breach of Kronos's security systems and data storage architecture in a timely manner;

(c) timely acting on all warnings and alerts, including public information, regarding Kronos's security vulnerabilities and potential compromise of the compiled data of Plaintiff;

(d) maintaining and implementing data security measures consistent with industry standards; and

(e) instituting data security policies and procedures, and adequately training employees and franchisees on such policies and procedures.

- Ultimate Kronos Group and Cargill Meat Solutions had common law duties to prevent foreseeable harm to Plaintiff.
- These duties existed because the Plaintiff was the foreseeable and probable victim of any inadequate security practices.
- In fact, not only was it foreseeable that Plaintiff would be harmed by the failure to protect his PII because hackers routinely attempt to steal such information and use it for nefarious purposes, Kronos knew that it was more likely than not Plaintiff would be harmed by such theft.
- Kronos had a duty to monitor, supervise, control, or otherwise provide oversight to safeguard the PII that was collected and stored on Kronos database systems.
- Kronos duties to use reasonable security measures also arose as a result of the special relationship that existed between Kronos and Cargill Meat Solutions on the one hand, and Plaintiff and other employees, on the other hand. The special relationship arose because the Plaintiff entrusted the Defendants with his PII in order to be an employee of Cargill Meat Solutions. Kronos alone could have ensured that its security systems and data storage architecture were sufficient to prevent or minimize the data breach.
- Kronos knew or should have known that its computer systems and data storage architecture were vulnerable to unauthorized access and targeting by hackers for the purpose of stealing and misusing confidential PII.
- Kronos and Cargill breached the duties it owed to Plaintiff described above and thus were negligent. Kronos breached these duties by, among other things, failing to:

(a) exercise reasonable care and implement adequate security systems, protocols and practices sufficient to protect the PII of Plaintiff;

(b) detect the breach while it was ongoing;

(c) maintain security systems consistent with industry standards; and

(d) institute data security policies and procedures, and adequately train employees and franchisees on such policies and procedures.

But for Kronos's wrongful and negligent breach of its duties owed to Plaintiff and the other Cargill employees, their PII would not have been compromised.

As a direct and proximate result of Cargill's and Kronos's negligence, Plaintiff has been injured and is entitled to damages in an amount to be proven at trial. Such injuries include one or more of the following: ongoing, imminent, certainly impending threat of identity theft crimes, fraud, and other misuse, resulting in monetary loss and economic harm; actual identity theft crimes, fraud, and other misuse, resulting in monetary loss and economic harm; loss of the value of his privacy and the confidentiality of the stolen PII; illegal sale of the compromised PII on the black market; mitigation expenses and time spent on credit monitoring, identity theft insurance, and credit freezes and unfreezes; time spent in response to the data breach reviewing bank statements, credit card statements, and credit reports; expenses and time spent initiating fraud alerts; decreased credit scores and ratings; lost work time; lost value of the PII; lost benefit of his employment; lost trust and confidence in his employer; and other economic and noneconomic harm.

THIRD CAUSE OF ACTION

Breach of Contract

Plaintiff incorporate by reference the allegations contained in each and every paragraph of this Complaint. At all relevant times, Cargill Meat Solutions and Cargill's employees mutually assented to and therefore were bound by the version of Kronos's Privacy Policy and Security Policy (the "Contract") that was operative at the time Plaintiff was employed by Cargill. Cargill stated on its website, in its "Cargill Data Privacy Principles" "We protect it against accidental or unlawful destruction or accidental loss, alteration, unauthorized disclosure or access, using appropriate technical and organizational measures." The contract was breached when the Plaintiff's Data was breached due to a "ransomware attack" on Kronos. The contract was also breached when the Plaintiff was not paid for actual hours worked.

Kronos's Privacy Policy forms a binding contract between Kronos and Cargill's employees. Cargill affirmatively stated in the Contract that it shares Employment Information with authorized Third-Party Service Providers, such as compensation and benefits providers that have a "need to know" that information. Where it does so, Cargill imposes appropriate contractual obligations regarding Employment Information on such Third-Party Providers.

Beyond our Third-Party Service Providers, generally, Cargill will only disclose your Employment Information outside Cargill and its Service Providers:

a) when required to do so by law;
b) in response to a legitimate request for assistance by the police or other law enforcement agency;
c) to seek legal advice from Cargill's external lawyers or in connection with litigation with a third party;
d) in connection with the sale, purchase or merger of a business; or
e) to provide a third party (such as a potential supplier or customer) with a means of contacting you in the normal course of business, for example, by providing your contact details, such as your business phone number and email address.

Cargill Meat Solutions and Ultimate Kronos Group breached the Contract by failing to have proper safeguards to protect the Plaintiff's PII and allowing a malicious third party to access that information without permission. The Defendants have violated its commitment to maintain the confidentiality and security of the PII of Plaintiff and failed to comply with their own polices and industry standards related to data security.

FOURTH CAUSE OF ACTION

Breach of the Implied Covenant of Good Faith and Fair Dealing

Plaintiff incorporate by reference the allegations contained in each and every paragraph of this Complaint. Plaintiff entered contracts with Cargill, the Privacy Policy, which included the implied terms that Cargill would not expose the PII to hackers and that Cargill would take reasonable measures to protect the PII. In this contract, as in every contract, there was an implied covenant of good faith and fair dealing. This implied promise means that each party will not do anything to unfairly interfere with the right of any other party to receive the benefits of the contract. Good faith means honesty of purpose without any intention to mislead or to take unfair advantage of another, that is, being faithful to one's duty or obligation.

Plaintiff performed everything that he was required to do under the contract by supplying his PII and working for Cargill Meat Solutions. All conditions for Kronos's performance have occurred or were excused. Kronos failed to protect the PII from exposure to hackers and failed to adopt reasonable measures to protect the PII, operating a website with numerous security flaws.

By doing so, Ultimate Kronos Group and Cargill Meat Solutions did not act fairly and in good faith. Good faith and fairness required Cargill and Kronos to protect the PII from hackers, including by adopting reasonable measures. Employees must count on companies who collect their PII to protect that PII in order to facilitate commercial transactions, which increasingly occur over the internet.

As a result of this conduct, the Plaintiff was damaged. Its more than likely the Plaintiff's and other Cargill employees' PII is being sold by nefarious individuals on the dark web. As a result, the Plaintiff has been forced to incur out of pocket costs for credit monitoring, and to take time and effort to cancel credit cards and/or freeze accounts. Plaintiff has also lost the benefit of their bargain. Plaintiff agreed to work for Cargill Meat Solutions and provide his PII to Cargill (whom shared the Plaintiff's PII with Kronos) with the understanding that his PII would be protected. Had the Plaintiff known that his PII would not be protected, he would not have agreed to be employed at Cargill Meat Solutions. The Plaintiff also face a significant risk that his PII will be stolen, that he will lose money, and that his identity will be stolen as a result of the breach. That risk only increases as time passes and no action is taken. Finally, Plaintiff and other Cargill's employees have lost the value of their PII, which has a real market value. Plaintiff has suffered monetary injury in fact as a direct and proximate result of the acts committed by Cargill Meat Solutions and Ultimate Kronos Group, as alleged herein, in an amount to be proven at trial, but in excess of the minimum jurisdictional amount of this Court. Cargill Meat Solutions, Ultimate Kronos Group and the Plaintiff entered an implied contract governing the use and protection of

PII when the Plaintiff supplied his PII in order to work for Cargill Meat Solutions. Plaintiff performed everything that he was required to do under the contract by supplying his PII. All conditions required for Kronos's performance have occurred or were excused. This contract was manifested in the conduct of the parties. By agreeing to take Plaintiff's PII into its possession, Kronos impliedly agreed to protect that PII from hackers, who were known to attempt to steal PII by hacking entities which possess it, to adopt reasonable measures to protect the PII from hackers, and to timely notify the Plaintiff of a data breach should one occur. Kronos knew, or had reason to know, that by taking the PII, it was engaging in conduct that would lead the Plaintiff to believe that Kronos would protect that data from exposure to hackers, due to the known risk of hacking, which was understood by all parties to the contract. Kronos breached these promises; thus, Cargill Meat Solutions breached these promises. As shown, Kronos allowed hackers to obtain Cargill's employees' PII. Kronos failed to adopt reasonable security measures to protect Cargill's employees' data.

As a result of these breaches, the Plaintiff and other Cargill's employees were damaged. Plaintiff's PII is possibly being sold by nefarious individuals on the dark web. As a result, the Plaintiff has been forced to incur out of pocket costs for credit monitoring, and to take time and effort to cancel credit cards and/or freeze accounts. The Plaintiff has also lost the benefit of his bargain. The Plaintiff agreed to work for Cargill provided his PII to Cargill with the understanding that his PII would be protected. Had the Plaintiff known that his PII would not be protected, he would not have agreed to be employed by Cargill Meat Solutions.

Plaintiff also face a significant risk that his PII will be stolen, that he will lose money, and that his identity will be stolen as a result of the breach. That risk only increases as time passes and no action is taken. Finally, Plaintiff has lost the value of his PII, which has a real market value.

The Plaintiff's losses were caused by Kronos's data breach. By allowing the hackers to obtain the PII, Kronos caused the Plaintiff and other Cargill employees to incur out-of-pocket expenses, lose the benefit of their agreement with Cargill, incur the risk of identity and property theft, and lose the value of their PII. The Plaintiff has suffered monetary injury in fact as a direct and proximate result of the acts committed by Cargill Meat Solutions and Ultimate Kronos Group, as alleged herein, in an amount to be proven at trial, but in excess of the minimum jurisdictional amount of this Court.

FIFTH CAUSE OF ACTION

Breach of the Implied Contract

Plaintiff incorporate by reference the allegations contained in each and every paragraph of this Complaint.

Plaintiff also entered into an implied contract with Cargill when he agreed to employment with Cargill, or otherwise provided PII to Cargill.

As part of these transactions, Cargill agreed to safeguard and protect the PII of Plaintiff.

The Plaintiff entered into implied contracts with the reasonable expectation that Kronos's data security practices and policies were reasonable and consistent with industry standards. Plaintiff believed that part of the monies paid by Cargill Meat Solutions to Kronos under the implied contracts to fund adequate and reasonable data security practices.

Plaintiff would not have provided and entrusted his PII to Cargill in the absence of the implied contract or implied terms between him and Cargill. The safeguarding of the PII of the Plaintiff was critical to realize the intent of the parties.

Plaintiff fully performed his obligations under the implied contracts with Cargill Meat Solutions.

Kronos breached its implied contract with the Plaintiff to protect his PII when it failed to have security protocols and measures in place to protect that information which resulted in a data breach. As a direct and proximate result of these breaches of implied contract, Plaintiff sustained actual losses and damages as described in detail above including, but not limited to, that he did not get the benefit of the bargain pursuant to which he provided his PII to Cargill.

As a result of these breaches, Plaintiff was damaged. Plaintiff's PII is being sold by nefarious individuals on the dark web. As a result, Plaintiff have been forced to incur out of pocket costs for credit monitoring, and to take time and effort to cancel credit cards and/or freeze accounts.

Plaintiff has also lost the benefit of his bargain. Plaintiff agreed to employment provided his PII to Cargill with the understanding that his PII would be protected. Had the Plaintiff known that their PII would not be protected, he would not have agreed to the employment contract. Plaintiff also face a significant risk that his PII will be stolen, that he will lose money, and that his identity will be stolen as a result of the breach. That risk only increases as time passes and no action is taken. Finally, the Plaintiff has lost the value of his PII, which has a real market value.

SIXTH CAUSE OF ACTION

Breach of Confidence

Plaintiff incorporate by reference the allegations contained in each and every paragraph of this Complaint.

Plaintiff conveyed confidential and novel information to Cargill Meat Solutions.

Cargill Meat Solutions and Ultimate Kronos Group had knowledge that the information was being disclosed in confidence.

There was an understanding between Cargill and the Plaintiff that the confidence would be maintained.

There was a data breach/disclosure in violation of the understanding.

As a result of these breaches, Plaintiff was damaged. Plaintiff's PII is possibly being sold by nefarious individuals on the dark web. As a result, Plaintiff have been forced to incur out of pocket costs for credit monitoring, and to take time and effort to cancel credit cards and/or freeze accounts. Plaintiff has also lost the benefit of his bargain. Plaintiff agreed to employment with Cargill and provided them with his Private Information with the understanding that his PII would be protected. Had Plaintiff known that his PII would not be protected, he would not have agreed to employment. Plaintiff also face a significant risk that his PII will be stolen, that he will lose money, and that his identity will be stolen as a result of the breach. That risk only increases as time passes and no action is taken. Finally, Plaintiff has lost the value of his PII, which has a real market value.

SEVENTH CAUSE OF ACTION

VIOLATION OF 29 C.F.R. 516.2

29 C.F.R. 516.2 states employers must generally keep accurate records of all hours worked for non-exempt employees (working "off the clock" is never allowed for non-exempt employees). The exact method of recording the time worked is up to the employer, but it must be in a form that can be made available. The defendant Cargill Meat Solutions violated this law by manipulating the plaintiff's timesheet record without his knowledge thus not paying him for his hours actually worked. This law was also violated when the employer failed to keep accurate records of all hours worked.

RELIEF REQUESTED

Plaintiff, on behalf of himself, requests the Court enter judgment against Cargill Meat Solutions and Ultimate Kronos Group as follows:

a) An order enjoining Defendants from further unfair and deceptive business practices regarding the maintenance and protection of Cargill's Employees' PII;

c) An award to Plaintiff for compensatory, punitive, exemplary, and statutory damages, including interest, in an amount to be proven at trial;

d) A declaration that the Defendants must make full restitution to Plaintiff;

e) An award of pre-judgment and post-judgment interest, as provided by law;

f) For an order certifying a collective action for the FLSA claims;

g) For an order finding Cargill Meat Solutions and Ultimate Kronos Group liable for violations of federal wage laws with respect to Ellis,

h) For a judgment awarding all unpaid wages, liquidated damages, and penalties, to Ellis;

i) For a judgment awarding costs of this action to Ellis;

j) For a judgment awarding pre- and post-judgment interest at the highest rates allowed by law to Ellis;

k) For all such other and further relief as may be necessary and appropriate.

DEMAND FOR JURY TRIAL

Pursuant to Federal Rule of Civil Procedure 38(b) Plaintiff demands a trial by jury of any and all issues in this action so triable.

Dated: September 26, 2022

Respectfully submitted,

Eric L Ellis

8539 Melissa Dr

Fort Worth, Tx 76108

3185075030

EricLamarEllis@gmail.com

9.26.2022