Margot Cutter (SBN 306789)
mcutter@cutterlaw.com
CUTTER LAW, PC
401 Watt Ave.
Sacramento, CA 95864
Telephone: 916.290.9400
Facsimile: 916.588.9314

Nicholas Andrew Hall (Texas Bar No. 24069863)*
HALL ATTORNEYS, PC
P.O. Box 1370
Edna, Texas 77957
Telephone: (713) 428-8967
Email: nhall@hallattorneys.com
**pro hac vice forthcoming*

Tina Wolfson (SBN 174806)
twolfson@ahdootwolfson.com
Jeff S. Westerman (SBN 94559)
jwesterman@ahdootwolfson.com
Lisa Cintron (SBN 356009)
lcintron@ahdootwolfson.com
AHDOOT & WOLFSON, PC
2600 W. Olive Ave., Suite 500
Burbank, California 91505
(310) 474-9111 (telephone)
(310) 474-8585 (facsimile)

Attorneys for Plaintiff and the Proposed Classes

UNITED STATES DISTRICT COURT
EASTERN DISTRICT OF CALIFORNIA
SACRAMENTO DIVISION

MAGEN MELISSA VENNOR, individually and on behalf of all others similarly situated,

Plaintiff,

v.

PAIDWORK LLC,

Defendant.

Case No. _____

CLASS ACTION COMPLAINT
1. Negligence
2. Breach of Implied Contract
3. Breach of Confidence
4. Restitution / Unjust Enrichment
5. Declaratory and Injunctive Relief

DEMAND FOR JURY TRIAL

Plaintiff Magen Melissa Vennor ("Plaintiff"), individually and on behalf of all others similarly situated, alleges the following against Defendant Paidwork LLC ("Paidwork" or "Defendant") upon personal knowledge as to herself and her own acts, and upon information and belief as to all other matters, after an investigation by counsel that is continuing:

NATURE OF THE ACTION

1. This putative class action arises from Paidwork's failure to use reasonable safeguards to protect the highly sensitive identity, credential, payment, and financial information that it collected and retained from millions of users, and from its failure to provide prompt and adequate notice after that information was accessed, acquired, exfiltrated, offered for sale, and ultimately disclosed publicly in a massive 2026 data breach (the "Data Breach").

2. Paidwork operates a global gig-economy and microtask platform through which users create accounts, perform online tasks, track earnings, and designate PayPal or bank-transfer information for withdrawals. To provide those services, Paidwork required or induced users to entrust it with personal and financial information, including names, email addresses, passwords, physical addresses, telephone numbers, dates of birth, device and IP information, payment information, and payout histories (collectively, "Private Information").

3. In or about March 2026, a threat actor claimed to have penetrated Paidwork's production environment and obtained approximately 11 gigabytes of data associated with tens of millions of users. The data was reportedly offered for sale by early April 2026 and was later posted publicly in July 2026.

4. Have I Been Pwned ("HIBP") reports that the compromised dataset contains approximately 23.3 million unique accounts and includes bank account numbers, dates of birth, device information, education levels, email addresses, financial transactions, genders, IP addresses, names, passwords stored as bcrypt hashes, personal interests, phone numbers, physical addresses, profile photographs, banking information, and worker payout histories.

5. HIBP notified Plaintiff on July 19, 2026 that her email address appeared in the Paidwork breach dataset. Plaintiff received that notice months after the March 2026 intrusion and after she had already suffered actual account takeover and financial misuse.

6. Beginning in the same month as the reported breach, Plaintiff experienced a cascade of identity- and account-takeover events. On March 31, 2026, PayPal notified her that a new PayPal account had been created using her name and restricted core features of her existing account. On May 27 and June 12, KOHO detected logins from an unrecognized device; the intruder changed the account email and caused unauthorized transfers and charges. Plaintiff currently has documentation of at least CAD $1,166.66 in unauthorized KOHO transactions, and the complete loss remains under investigation. On July 20, 2026, she reported the identity theft and account takeovers to the Federal Bureau of Investigation's Internet Crime Complaint Center ("IC3").

7. On information and belief, the chronology and attack pattern are consistent with misuse of data exposed in the Paidwork Data Breach. Plaintiff used the same password for Paidwork and other online accounts; HIBP later confirmed her Paidwork email address in the corpus; and the corpus reportedly contained password hashes, bank-account numbers, financial-transaction histories, email addresses, device information, phone numbers, physical addresses, and other identity data that can be combined to conduct credential-stuffing, account-recovery, and social-engineering attacks.

8. Paidwork's failure to provide prompt notice independently magnified the harm. Had Paidwork disclosed the Data Breach at or near the time it occurred or was offered for sale, Plaintiff could have—and, consistent with her documented history of vigilant self-protection, would have—immediately hardened or replaced the banking, payment, email, and telecommunications credentials associated with the exposed data before they were exploited.

9. Plaintiff brings this action to recover compensatory, restitutionary, nominal, and other available relief; to obtain appropriate declaratory and injunctive relief; to require Paidwork to remediate the security and notification failures that caused the Data Breach; and to protect the Class from continuing misuse of data that cannot simply be recalled or made private again.

PARTIES

10. Plaintiff Magen Melissa Vennor is a citizen of Canada and is domiciled in and resides in Edmonton, Alberta, Canada.

11. Defendant Paidwork LLC is a limited liability company that owns, operates, controls, and/or is responsible for the Paidwork website, mobile applications, user-account systems, payout functions, databases, and privacy and cybersecurity practices at issue.

12. Paidwork LLC is organized under the laws of California with its principal place of business located at 3400 Cottage Way, Suite G2 #27204, Sacramento, California 95825. Paidwork LLC identifies Sacramento as the place for dispute resolution under its currently posted terms.

13. Paidwork's exact corporate structure, members, managers, affiliates, database owners, responsible operating entities, and CAFA citizenship facts are peculiarly within Defendant's knowledge. Plaintiff reserves the right to amend this Complaint to conform the jurisdictional allegations and to add or substitute related entities and responsible parties as discovery warrants.

JURISDICTION AND VENUE

14. This Court has original subject-matter jurisdiction under the Class Action Fairness Act of 2005 ("CAFA"), 28 U.S.C. section 1332(d).

15. On information and belief, the proposed Classes contain far more than 100 members, satisfying 28 U.S.C. § 1332(d)(5)(B). HIBP reports approximately 23.3 million compromised accounts worldwide, and Paidwork offered its services throughout the United States and Canada. Paidwork's own records will establish the precise number and citizenship of North American Class members.

16. The aggregate amount in controversy exceeds $5,000,000, exclusive of interest and costs. Among other relief, Class members seek actual damages for financial misuse, loss of funds, mitigation expenses and time, loss of data value and privacy, restitution, nominal damages where available, and the value of classwide injunctive relief. The claims of individual Class members are aggregated under 28 U.S.C. § 1332(d)(6).

17. Minimal diversity exists under 28 U.S.C. § 1332(d)(2)(B). Plaintiff is a citizen of Canada and a member of both proposed Classes, and Paidwork is, on information and belief, a citizen of one or more States within the United States. CAFA expressly defines "class members" to include named and unnamed persons who fall within the proposed class definition. 28 U.S.C. § 1332(d)(1)(D).

18. For CAFA purposes, an unincorporated association such as Paidwork LLC is deemed a citizen of the State in which it has its principal place of business and the State under whose laws it is organized. 28 U.S.C. § 1332(d)(10). Neither Federal Rule of Civil Procedure 23 nor CAFA requires a named class representative to be a United States citizen or resident.

19. On information and belief, no mandatory CAFA exception applies. The proposed Classes are geographically dispersed, the claims arise from a breach affecting users across the United States and Canada, and the principal injuries were not confined to California.

20. Plaintiff has Article III standing. She alleges completed and concrete injuries, including unauthorized creation or attempted use of a PayPal account in her name; restriction and loss of functionality of her existing PayPal account; repeated email-account recovery attacks; unauthorized access to and takeover of her KOHO account; at least CAD $1,166.66 in documented unauthorized transfers and charges; an unresolved negative balance and resulting collection and credit risk; replacement of her telephone number and device; credit-monitoring, identity-protection, and fraud-alert expenses and burdens; extensive mitigation time; and continuing exposure to misuse of data that Paidwork allegedly continues to retain. Those injuries are traceable to the alleged security and notification failures and are redressable through damages and appropriate equitable relief.

21. This Court may grant declaratory and further relief under 28 U.S.C. sections 2201 and 2202 and has authority to award the legal and equitable remedies requested below.

22. This Court has personal jurisdiction over Paidwork because Paidwork publicly holds itself out as located in Sacramento, purposefully directs its services to residents of this District and users worldwide from U.S.-based operations, states that data of non-U.S. users may be transferred to, stored in, or processed in the United States, and, on information and belief, made or directed the challenged cybersecurity, data-retention, incident-response, and notification decisions in this District or elsewhere in the United States.

23. Paidwork has also deliberately invoked California law and selected Sacramento, California as the location for dispute resolution in its currently posted Terms of Service. Plaintiff does not concede that she assented to those post-breach terms or their arbitration provision, but Paidwork's own forum selection confirms substantial, purposeful contacts with Sacramento and California.

24. Venue is proper in this District under 28 U.S.C. § 1391(b)(1) and (2) because Paidwork identifies a registered address in Sacramento and, on information and belief, resides in this District for venue purposes, and because a substantial part of the acts and omissions giving rise to the claims - including data governance, security, retention, incident response, and notification decisions - occurred in or were directed from this District.

25. Intradistrict assignment to the Sacramento Division is proper under Eastern District of California Local Rule 120(d) because Defendant identifies a Sacramento County address and the claims arise, in substantial part, from conduct occurring in or directed from Sacramento County.

FACTUAL ALLEGATIONS

A. Paidwork collected high-risk credential, identity, and financial information

26. Paidwork markets itself as an online earning platform available to users around the world. Users can play games, complete surveys, watch videos, perform tasks, and engage with offers in exchange for purported earnings.

27. To use Paidwork, users create an account and provide an email address and password. Paidwork's current Privacy Policy states that Paidwork collects names, email addresses, passwords, payment information used to facilitate PayPal or bank-transfer withdrawals, device and usage information, IP addresses, and information obtained from payment providers and banks.

28. Paidwork's current Terms likewise state that withdrawals are made through bank transfer and PayPal and that its account systems track users, tasks, earnings, and payout information.

29. Paidwork knew that the Private Information it collected was highly sensitive. Payment-account identifiers, bank information, email addresses, dates of birth, physical addresses, phone numbers, IP and device data, payout histories, and password hashes can be combined to commit account takeover, credential stuffing, targeted phishing, identity fraud, financial fraud, and social-engineering attacks.

30. Paidwork also knew or should have known that many ordinary consumers reuse passwords across multiple services and that exfiltration of even hashed passwords creates a foreseeable risk when passwords are weak, reused, or susceptible to offline cracking. Credential reuse

is a known reason why a breach of one service can lead to compromise of email, payment, and banking accounts elsewhere.

31. Users did not provide their Private Information for sale, criminal use, or public distribution. They entrusted it to Paidwork for the limited purposes of creating and authenticating accounts, tracking tasks and purported earnings, processing withdrawals, preventing fraud, and administering the platform.

32. Paidwork benefited commercially from collecting and retaining this information. The information enabled Paidwork to operate its platform, authenticate and profile users, track engagement, process or market payout functions, attract business partners and advertisers, and avoid the costs of repeatedly recollecting user data.

33. Because Paidwork chose to collect and retain credential and financial information at enormous scale, it had a corresponding duty to use security measures commensurate with the sensitivity, volume, and foreseeable criminal value of that information.

B. Paidwork represented that it would secure and responsibly use user information

34. Paidwork's current Privacy Policy, effective March 29, 2026, states that Paidwork uses information to authenticate identity, process withdrawals, secure the platform, detect and prevent unauthorized access and fraudulent transactions, and comply with legal obligations.

35. That policy further states that Paidwork implements "robust security measures," including encryption, firewalls, and secure data storage, to protect user information. It also states that Paidwork will provide notice of material policy changes as required by law.

36. Plaintiff does not presently rely on the March 29, 2026 policy as the sole source of her contractual rights because her account was created earlier. Paidwork's historical policies and signup representations are within Defendant's possession and must be preserved and produced. The current policy nevertheless reflects Paidwork's own acknowledgment that the information required robust security and fraud-prevention controls during the relevant period.

37. Reasonable security for a platform retaining credential and financial data at Paidwork's scale required, at minimum, appropriate data minimization and retention; strong access controls and multifactor authentication for privileged systems; least-privilege permissions; network and database

segmentation; encryption and key management; secure password hashing parameters; vulnerability management and patching; logging, monitoring, and anomaly detection; intrusion detection and prevention; secure backup and exfiltration controls; employee and vendor security; incident-response testing; and prompt notice sufficient to permit users to protect themselves.

38. On information and belief, Paidwork failed to implement one or more of these controls adequately. The precise intrusion vector, dwell time, systems accessed, data tables exfiltrated, and security-control failures are exclusively or predominantly within Paidwork's possession and will be established through discovery and expert analysis.

39. Paidwork's deficient security and incident response were not excused by the criminal conduct of third parties. Cyber intrusion, credential theft, database exfiltration, sale of user records, credential cracking, and account takeover are foreseeable consequences of maintaining a large repository of payment, identity, and credential information without reasonable safeguards.

C. Threat actors obtained and disseminated Paidwork user data

40. In March 2026, a threat actor claimed to have obtained data from Paidwork's production systems. Public reporting in early April described an auction involving approximately 22 million user records and a sample containing emails, password hashes, names, addresses, device and location information, partial banking details, and payment-platform information.

41. By no later than April 2, 2026, Paidwork had been contacted by a news organization concerning the asserted breach and sale.

42. In July 2026, approximately 11 gigabytes of data attributed to Paidwork was reportedly posted publicly rather than remaining available only to a private seller or buyer. Public release materially increased the duration and breadth of the risk because any person with access to the dataset could copy, analyze, redistribute, and weaponize it.

43. HIBP added the Paidwork incident to its breach database and reported approximately 23.3 million affected accounts. HIBP identified the compromised data categories as bank account numbers, dates of birth, device information, education levels, email addresses, financial transactions, genders, IP addresses, names, passwords, personal interests, phone numbers, physical addresses, and profile photographs.

44. HIBP further described the dataset as including user-profile data, banking information, worker payout history, and passwords stored as bcrypt hashes. Although bcrypt is designed to impede rapid guessing, a stolen hash can still be attacked offline, particularly where the underlying password is weak or reused.

45. The exposed fields are especially dangerous in combination. Email, password, device, address, telephone, birth-date, payment, and transaction information can be correlated to defeat account-recovery controls, answer identity-verification questions, impersonate users, target phishing, open or access payment accounts, and launder or redirect funds.

46. Paidwork has not provided Plaintiff with a complete explanation of the incident, including when the intrusion began, when it ended, when Paidwork discovered it, which systems were accessed, what safeguards failed, which specific fields from Plaintiff's record were taken, who received the information before public release, or what steps Paidwork took to prevent misuse.

D. Plaintiff entrusted Paidwork with information of the kind later exploited

47. Plaintiff registered her Paidwork account in approximately 2024 under her email address and, in connection with the account and its payout functionality, supplied Paidwork with personal information of the kinds compromised in the Data Breach, including at least an email address, password, and PayPal account for payments.

48. Plaintiff used the same password for Paidwork and other online accounts. Like many consumers, she did so for memorability and convenience. Plaintiff does not disclose the password or its composition in this public pleading. After the takeover, she changed her credential practices and began using a password manager.

49. HIBP notified Plaintiff on July 19, 2026 that her Paidwork email address was present in the breach dataset. HIBP reported that the corpus included bank-account numbers, financial transactions and payout histories, email addresses, passwords stored as bcrypt hashes, device information, IP addresses, names, dates of birth, phone numbers, physical addresses, and other profile information.

50. On information and belief, the exfiltrated Paidwork records associated users' account identities with credential, banking, transaction, and payout information. Paidwork therefore placed

Plaintiff at foreseeable risk that an attacker could correlate her Paidwork email and reused password with her financial, payment, email, and telecommunications accounts.

51. Before the account activity described below, Plaintiff had not received a warning from Paidwork that its user database, password hashes, bank-account information, financial-transaction histories, or payment-related records had been accessed, offered for sale, or publicly disseminated.

52. Timely notice mattered. Had Paidwork promptly disclosed the Data Breach at or near the time it occurred or was offered for sale, Plaintiff could have—and, consistent with her documented history of vigilant self-protection, would have—immediately hardened or replaced the banking, payment, email, and telecommunications credentials associated with the exposed data before they were exploited.

53. Plaintiff had no practical means to discover Paidwork's internal compromise herself. Paidwork controlled the relevant systems, logs, and incident information and was the only party positioned to warn her that the credential, identity, banking, and transaction data she had entrusted to the platform was at risk.

E. Unauthorized account activity began in March 2026

54. On March 31, 2026, during the same month as the reported Data Breach, PayPal notified Plaintiff that "there's a new PayPal account that's been created using your name." Plaintiff did not create the duplicate account. PayPal restricted core features of Plaintiff's existing account pending re-verification of her identity, address, card, and banking details.

55. The restrictions persisted for weeks. On April 28, 2026, PayPal sent Plaintiff, at the same Outlook address later identified in the Paidwork dataset, a reminder stating, "It looks like someone was trying to use your PayPal account without your permission," and advised that her ability to send, receive, withdraw, and pay was paused until she uploaded photo identification and changed her password. PayPal sent a further reminder on May 15, 2026.

56. Between late March and mid-April 2026, Plaintiff's Microsoft accounts were also subjected to repeated account-recovery attempts, password-reset events, and security alerts. The activity required Plaintiff to repeatedly re-secure those accounts, including changing a recovery email and removing a passkey on April 13, 2026. Paidwork had not notified her of the Data Breach, so she

did not know that her Paidwork credentials and other exposed information could be part of the attack pattern.

F. Plaintiff suffered a coordinated KOHO account takeover and financial misuse

57. On May 27, 2026, KOHO—the Canadian financial-services platform at which Plaintiff held a deposit account—alerted Plaintiff to a login from a new device: an Android 14 device identified as model SM-A042F. Plaintiff has never owned or used that device. Her devices at the relevant times were an Apple iPhone and, beginning in mid-June 2026, a Samsung Galaxy S26+, which is a different model.

58. On May 28, 2026, at approximately 6:26 a.m. local time, an international transfer of CAD $977.17 was initiated from Plaintiff's KOHO account to a recipient identified as "Guillermo Fernandez Martinez." Plaintiff did not initiate or authorize the transfer and does not know that individual.

59. On June 12, 2026, the takeover escalated in a coordinated sequence. At approximately 5:07 a.m. local time, KOHO alerted Plaintiff to another login from the same unverified Android device. At approximately 5:18 a.m., the email address on the account was changed away from Plaintiff's control. At approximately 5:42 a.m., a CAD $35.00 Interac e-Transfer was sent to "Panda Digital Media Limited." At approximately 6:09 a.m. and 6:12 a.m., charges of CAD $3.81 and CAD $150.68 were made to the Skrill money-transfer service. Plaintiff authorized none of these transactions or account changes.

60. Plaintiff detected the June 12 activity in real time, demanded an emergency lock on her account within minutes, and reported the fraudulent Interac transfer to Interac's anti-phishing address within approximately five minutes of its occurrence. Because the intruder had changed the email address on the account, KOHO's support personnel initially could not locate Plaintiff's account using her identifying information, causing a delay directly attributable to the takeover.

61. KOHO locked the account on June 14, 2026, stating that it did so "to prevent any further unauthorized access." Plaintiff formally disputed the unauthorized transactions, opened in-app disputes that remain under review, and, on June 16, 2026, escalated the matter in writing to compliance personnel at Peoples Group, KOHO's issuing institution. She requested a regulator-

compliant final position letter and the session, IP-address, and device records associated with the intrusion. Plaintiff also escalated the matter to the Ombudsman for Banking Services and Investments and reported it to the Canadian Anti-Fraud Centre and law enforcement.

62. The itemized unauthorized transactions documented to date total CAD $1,166.66. On information and belief, Plaintiff's total loss and exposure are higher: KOHO's fraud personnel acknowledged Plaintiff's report that all funds in the account had been transferred out, and complete itemization awaits KOHO's production of account records.

63. As of July 12, 2026, KOHO was demanding that Plaintiff pay a balance created by the intrusion. Plaintiff disputes that balance. The demand exposes her to collection activity and credit harm for sums she did not spend or authorize.

64. On July 20, 2026, Plaintiff filed an IC3 complaint regarding the identity theft and account takeovers. Based on the information then available, she estimated her total loss at approximately $4,000. Her current records document at least CAD $1,166.66 in itemized unauthorized KOHO transactions, while the complete amount of loss, loss of use, fees, and disputed balance remains subject to KOHO's records and the pending disputes.

65. In response, Plaintiff has undertaken extensive, documented mitigation. Among other things, she replaced her mobile telephone number; replaced her mobile device and migrated device platforms; repeatedly rotated passwords, passkeys, and recovery credentials across financial, email, and platform accounts; maintained credit-monitoring and identity-protection services; maintained a fraud alert with a national credit bureau; filed and prosecuted disputes and complaints with financial institutions, a payment network, a federal complaints body, an ombudsman, law-enforcement agencies, and anti-fraud agencies in two countries; and devoted dozens of hours—and, on some days, dozens of communications—to securing her accounts and documenting the intrusions.

66. Plaintiff has not been made whole. She continues to face unresolved financial disputes, a negative or impaired account balance, potential collection and credit consequences, loss of use of funds and account functionality, out-of-pocket mitigation costs, loss of privacy and control over her Private Information, and continuing risk of further fraud, identity theft, phishing, credential attacks, and financial misuse.

G. Paidwork's delayed notice magnified the harm

67. On information and belief, the criminals who took over Plaintiff's KOHO account knew to target it—and possessed identity, contact, credential, banking, and transaction information useful to do so—because that information was contained in or derived from the Paidwork database stolen in the Data Breach. At present, among the breaches reflected in Plaintiff's HIBP history, the Paidwork corpus is the only one Plaintiff has identified as confirmed to contain both bank-account numbers and financial-transaction histories.

68. The timing and sequence reinforce that inference. The attempted new-account and account-recovery activity began in the same month as the reported Data Breach, continued after the dataset was offered for sale, and escalated into the KOHO takeover while Paidwork's stolen data remained available to criminals. The overlap between the compromised fields and the information used in the attacks further supports traceability at the pleading stage.

69. A threat actor who recovered or matched Plaintiff's reused credential, or combined the credential hash with the exposed identity, device, address, telephone, banking, payout, and transaction information, could use credential-stuffing, account-recovery, or social-engineering techniques to access related email, payment, and financial accounts. The intervening criminal acts were the very risks that reasonable data security and prompt breach notice were intended to prevent.

70. Plaintiff learned that her Paidwork account was included in the breach only through HIBP on July 19, 2026. By then, the PayPal restrictions, email-account attacks, KOHO takeover, unauthorized transactions, and substantial mitigation burden had already occurred. Paidwork's discovery date, investigation timeline, communications with the threat actor, insurers, vendors, law enforcement, regulators, HIBP, and affected users, and any asserted reasons for delay remain within Paidwork's exclusive possession.

H. The risk and need for remediation remain ongoing

71. Private Information such as names, birth dates, addresses, telephone numbers, transaction histories, bank-account information, profile photographs, and credential data cannot be reissued in the same way as a payment card. Once disclosed publicly, it can be copied indefinitely and used in future attacks.

72. Plaintiff and Class members remain at heightened risk of credential stuffing, phishing, account recovery abuse, new-account fraud, payment diversion, bank and PayPal fraud, identity theft, doxing, and targeted scams. Actual misuse suffered by Plaintiff confirms that the risk is not hypothetical.

73. Paidwork continues to possess Private Information belonging to Plaintiff and Class members. Without court-ordered transparency and remediation, Class members cannot determine whether Paidwork has corrected the vulnerabilities, minimized unnecessary retention, reset or invalidated exposed credentials, restricted compromised payout identifiers, or implemented monitoring adequate to prevent recurrence.

I. Plaintiff did not agree to Paidwork's arbitration and class-waiver terms

74. Paidwork's currently posted Terms of Service state that they were last updated April 16, 2026—after Plaintiff joined Paidwork in approximately 2024 and after the alleged March 2026 Data Breach.

75. Those current terms contain a California choice-of-law clause, a provision requiring AAA arbitration in Sacramento, and a purported class-action and class-arbitration waiver. They also state that significant changes will be communicated by email or website notice and that continued use constitutes acceptance.

76. Plaintiff did not knowingly or affirmatively agree to the April 16, 2026 arbitration provision or class waiver. She did not receive conspicuous notice identifying the new arbitration and class-waiver terms and did not unambiguously manifest assent to them.

77. Plaintiff's claims arise from Paidwork's independent duties to protect Private Information and provide reasonable incident response and from a breach that occurred before the April 16 terms. Paidwork cannot manufacture retroactive assent to arbitration or a class waiver through an undisclosed, post-breach website revision.

78. Plaintiff anticipates that Paidwork may invoke the current terms but denies that any enforceable agreement to arbitrate this dispute exists. The formation, version, notice, and assent issues must be decided by the Court before any purported arbitration rules or delegation provision can apply.

CLASS ACTION ALLEGATIONS

79. Plaintiff brings this action under Federal Rules of Civil Procedure 23(a), 23(b)(2), and 23(b)(3), individually and on behalf of the following proposed class and subclass, subject to amendment after discovery:

> **North American Data Breach Class**: All persons residing in the United States or Canada whose Private Information was accessed, acquired, exfiltrated, stolen, compromised, or publicly disclosed as a result of the Paidwork Data Breach.
>
> **Actual Misuse Subclass**: All members of the North American Data Breach Class who experienced actual or attempted unauthorized access to, opening of, or transactions through a financial, payment, email, or other online account that was caused by or reasonably traceable to the Paidwork Data Breach.

80. Plaintiff is a member of both proposed Classes. She resides in Canada, her Private Information was included in the Paidwork breach dataset, and she experienced actual and attempted unauthorized opening of and actual unauthorized access to payment, email, and financial accounts—including a duplicate PayPal account created in her name and the takeover of her KOHO account—which she alleges were caused by or reasonably traceable to the Data Breach.

81. Excluded from the Classes are Paidwork and its parents, subsidiaries, affiliates, officers, directors, members, managers, and employees; any entity in which Paidwork has a controlling interest; the judges and court personnel assigned to this case and their immediate family members; and any person who validly requests exclusion from a Rule 23(b)(3) class.

82. Plaintiff reserves the right to amend, narrow, or create additional U.S., state, provincial, consumer, financial-information, credential-exposure, and actual-misuse subclasses after discovery and to add additional qualified representatives as appropriate. Additional U.S. or state-specific representatives may strengthen particular statutory or choice-of-law subclasses, but they are not a prerequisite to Plaintiff's commencement of this action on behalf of the Classes defined above.

83. Numerosity. The Classes are so numerous that joinder is impracticable. The breach reportedly involved approximately 23.3 million unique accounts. On information and belief, more

than 100 affected users reside in the United States or Canada, and the precise North American count is ascertainable from Paidwork's account, breach, notification, payout, and database records.

84. Commonality. Common questions of law and fact include:

A. whether Paidwork owed duties to use reasonable security and incident-response practices;

B. whether and when unauthorized actors accessed, acquired, or exfiltrated Paidwork data;

C. which systems, tables, records, and data fields were compromised;

D. whether Paidwork's security architecture, access controls, monitoring, retention, password protections, vendor management, and incident response were reasonable;

E. when Paidwork discovered or reasonably should have discovered the Data Breach;

F. whether Paidwork provided timely and adequate notice;

G. whether Paidwork's conduct caused or increased the risk of credential stuffing, account takeover, payment fraud, and identity theft;

H. whether an implied contract or confidential relationship required Paidwork to safeguard Private Information and provide prompt notice;

I. whether Paidwork was unjustly enriched by collecting and retaining user data while avoiding reasonable security expenditures;

J. whether Plaintiff and Class members are entitled to damages, restitution, declaratory relief, and injunctive relief; and

K. whether Paidwork's April 16, 2026 arbitration and class-waiver terms were effectively communicated to and accepted by preexisting users.

85. Typicality. Plaintiff's claims arise from the same course of conduct as the claims of the Classes: Paidwork collected and retained her Private Information, failed to protect it, failed to warn her promptly, and exposed her to the same categories of credential, identity, banking, and transaction misuse. Her Canadian citizenship and residence do not alter the common security, breach-response, notice, causation, and remediation questions. Plaintiff also suffered the completed and attempted account misuse that defines the Actual Misuse Subclass.

86. Adequacy. Plaintiff will fairly and adequately protect the interests of the Classes. She is a member of both proposed Classes, her interests are aligned with those of other affected users, she has no known disabling conflict, she understands her obligation to participate in discovery and protect absent members, and she has retained counsel experienced in class and data-breach litigation. Plaintiff is willing and able to participate in discovery and proceedings in the United States. Her Canadian citizenship and residence create no inherent conflict with U.S. Class members.

87. Predominance. Common liability questions concerning Paidwork's systems, safeguards, breach response, notice, data practices, and uniform conduct predominate over individualized issues. Differences in damages or applicable law do not defeat the common liability case and can be addressed, as necessary, through subclasses, issue certification under Rule 23(c)(4), damages methodologies, and claims administration.

88. Superiority. A class action is superior to thousands or millions of separate actions because individual damages may be too small to justify standalone litigation, the relevant security evidence is concentrated in Paidwork's possession, and common adjudication will promote efficiency and consistent results.

89. Rule 23(b)(2). Paidwork has acted or refused to act on grounds generally applicable to the Classes by maintaining common data systems, security practices, retention policies, and incident-response procedures. Declaratory and injunctive relief respecting those systems is appropriate for the Classes as a whole.

90. Ascertainability. Class membership is administratively feasible and objectively determinable from Paidwork's affected-user records, breach dataset, account databases, notification files, payout records, and records of reported actual misuse.

91. Manageability. The Court can sequence common liability issues before individualized damages, use U.S., state, provincial, or injury-based subclasses where substantive law materially differs, and certify issues under Rule 23(c)(4) or subclasses under Rule 23(c)(5) as appropriate. Plaintiff anticipates adding U.S. and state-specific representatives where doing so will assist certification of particular claims, but no such addition is necessary to establish Plaintiff's standing or to commence this action.

GOVERNING LAW AND CLASS ARCHITECTURE

92. Plaintiff pleads the common-law claims below under the law the Court determines governs her claims and the claims of materially similar Class members. Plaintiff does not contend that one jurisdiction's law must govern every Class member if California choice-of-law rules require otherwise; she requests subclasses, issue certification, or other appropriate case-management measures where material differences in governing law exist.

TOLLING AND DELAYED DISCOVERY

93. Any applicable limitations periods were tolled by the delayed discovery rule because Paidwork controlled the relevant systems and incident information, the intrusion and exfiltration were inherently undiscoverable to ordinary users, and Plaintiff did not learn that her Paidwork account appeared in the breach dataset until HIBP notified her on July 19, 2026.

94. To the extent Paidwork knew of the intrusion or sale before providing notice, its failure to disclose material facts concerning the Data Breach prevented Plaintiff and Class members from discovering their claims and supports equitable tolling and estoppel.

95. Plaintiff and Class members acted reasonably. They had no practical means to inspect Paidwork's internal databases, logs, security alerts, incident reports, or communications with threat actors and could not have discovered the relevant security failures through ordinary diligence.

COUNT I
NEGLIGENCE
(On Behalf of Plaintiff and the Classes)

96. Plaintiff incorporates the preceding allegations as though fully set forth here.

97. Paidwork owed Plaintiff and Class members a duty to exercise reasonable care in collecting, storing, securing, using, retaining, and deleting their Private Information and in detecting, investigating, containing, and providing notice of unauthorized access.

98. The duty arose from Paidwork's affirmative collection and custody of sensitive information; the special relationship created when users entrusted credential and financial data for account and payout purposes; Paidwork's superior knowledge and control; the foreseeability of criminal misuse; Paidwork's representations and undertakings; generally accepted cybersecurity practices; and applicable statutory and regulatory standards that inform reasonable care.

99. Paidwork had a duty to use safeguards proportionate to the volume and sensitivity of the data, to test and monitor those safeguards, to minimize and securely dispose of unnecessary information, to limit and audit access, to protect credential and payment data, to maintain an effective incident-response plan, and to warn users promptly when a breach created a foreseeable risk of credential and financial-account misuse.

100. Paidwork breached those duties by, among other things, failing to implement or maintain reasonable access controls, segmentation, monitoring, vulnerability management, exfiltration detection, credential protections, encryption and key management, data minimization, vendor controls, incident-response procedures, and timely notification; retaining sensitive information longer or more broadly than reasonably necessary; and failing to act promptly after the breach was or should have been discovered.

101. Paidwork's breaches caused and substantially contributed to the unauthorized access, acquisition, dissemination, and misuse of Private Information and deprived Plaintiff and Class members of the opportunity to mitigate foreseeable harm.

102. The account-takeover and financial misuse suffered by Plaintiff were foreseeable consequences of exposing credential and payment-related data and delaying notice. The intervening criminal acts were the very risks that reasonable data security and incident response were required to guard against.

103. Plaintiff and Class members suffered damages including actual financial loss and loss of use of funds; unauthorized account creation, access, and transactions; impaired or negative account balances; fees; collection and credit risk; replacement of telephone numbers and devices; credit-monitoring, identity-protection, and fraud-alert expenses and burdens; extensive mitigation time; loss of account functionality, access, and control; loss of privacy and confidentiality; diminished value of Private Information; and continuing risk requiring monitoring and protective measures.

104. As a direct and proximate result, Plaintiff and the Classes are entitled to compensatory, nominal, consequential, and other damages available under the governing law, together with appropriate equitable relief.

COUNT II
BREACH OF IMPLIED CONTRACT
(On Behalf of Plaintiff and the Classes)

105. Plaintiff incorporates the preceding allegations as though fully set forth here.

106. When Plaintiff and Class members created Paidwork accounts and supplied Private Information, the parties formed an implied contract. Plaintiff and Class members agreed to provide account credentials, profile data, engagement, labor or task activity, and payout information for Paidwork's limited business purposes; Paidwork implicitly agreed to use the information only for

those purposes, apply reasonable security, and provide reasonably prompt notice of a breach so users could protect themselves.

107. The security and notice promises were material because no reasonable user would knowingly provide credential and financial information to a platform that intended to store it without reasonable safeguards or remain silent while attackers sold or weaponized it.

108. Plaintiff and Class members performed by creating and maintaining accounts, providing information, engaging with Paidwork's platform, and conferring the commercial benefits described above. Plaintiff's failure to receive a payout does not eliminate the exchange or Paidwork's duty to protect the data it chose to retain.

109. Paidwork breached the implied contract by failing to safeguard Private Information, allowing it to be accessed and exfiltrated, failing to contain and remediate the incident reasonably, and failing to provide timely and adequate notice.

110. Paidwork's breach caused Plaintiff and Class members the damages and injuries described above. Plaintiff seeks contract damages and other relief available under the governing law.

COUNT III
BREACH OF CONFIDENCE
(On Behalf of Plaintiff and the Classes)

111. Plaintiff incorporates the preceding allegations as though fully set forth here.

112. Plaintiff and Class members conveyed Private Information to Paidwork in confidence and for limited purposes related to account administration, authentication, task activity, fraud prevention, and withdrawals. This claim is asserted to the extent recognized under the governing law applicable to Plaintiff and any materially similar Class members.

113. The nature of the information and Paidwork's role created a reasonable understanding that Paidwork would maintain confidentiality, restrict access, and not permit the information to be disclosed to unauthorized actors or the public.

114. Paidwork accepted the information under those circumstances and knew or should have known that unauthorized disclosure would create a serious risk of identity, credential, and financial harm.

115. Paidwork breached that confidence by failing to maintain reasonable controls and permitting Private Information to be accessed, acquired, offered for sale, and publicly disclosed outside the purposes for which it was entrusted.

116. Plaintiff and Class members were injured as a direct and proximate result and are entitled to damages, restitution, and equitable relief available under the governing law.

COUNT IV
RESTITUTION / UNJUST ENRICHMENT
(On Behalf of Plaintiff and the Classes; Pleaded in the Alternative)

117. Plaintiff incorporates the preceding allegations as though fully set forth here.

118. Paidwork received and retained valuable benefits from Plaintiff and Class members, including their Private Information, account registrations, attention, engagement, labor or task activity, data used to operate and monetize the platform, and the cost savings obtained by retaining information for future use.

119. Paidwork also retained the benefit of security expenditures it should have made but avoided, while shifting the costs and risks of deficient security and delayed notice to users whose data it collected.

120. It would be unjust for Paidwork to retain those benefits without compensating affected users or funding adequate remediation after failing to provide the reasonable security and incident response that formed part of the exchange.

121. To the extent no enforceable contract governs, Plaintiff and the Classes seek restitution, disgorgement of benefits wrongfully retained, and other equitable monetary relief permitted by law. This Count is pleaded in the alternative and does not seek duplicative recovery.

COUNT V
DECLARATORY AND INJUNCTIVE RELIEF
(On Behalf of Plaintiff and the Classes)

122. Plaintiff incorporates the preceding allegations as though fully set forth here.

123. An actual and continuing controversy exists concerning Paidwork's duties, the reasonableness of its data-security and notification practices, the continued retention of compromised information, and the measures required to reduce ongoing risk.

124. Money damages alone are inadequate because the dataset has reportedly been publicly distributed, the exposed identity and financial information cannot all be changed, Paidwork continues to possess user information, and Class members face continuing risk of account takeover, identity theft, payment fraud, and targeted attacks.

125. Plaintiff seeks a declaration that Paidwork owed and breached duties to use reasonable security and provide reasonable incident response and notice, and that Paidwork must protect, minimize, and remediate the compromised information consistent with law and reasonable cybersecurity practice.

126. Plaintiff further seeks an injunction requiring, as appropriate after discovery: an independent security assessment; remediation of identified vulnerabilities; reasonable access controls, monitoring, segmentation, credential protection, and incident response; data minimization and secure deletion; identification of affected data fields; adequate individualized notice; monitoring for misuse of exposed credentials and payout identifiers; reasonable identity and account-protection services; and periodic compliance reporting to the Court or an independent assessor.

127. The requested relief is narrowly directed to the continuing risks created by Paidwork's common systems and conduct and will benefit the Classes as a whole.

PRAYER FOR RELIEF

WHEREFORE, Plaintiff, individually and on behalf of the proposed Classes, respectfully requests that the Court enter judgment in her favor and against Paidwork and award the following relief:

A. Certify the proposed Classes under Federal Rule of Civil Procedure 23 and any appropriate subclasses or issues; appoint Plaintiff as class representative; and appoint her counsel as class counsel;

B. Declare that Paidwork's acts and omissions alleged herein were wrongful and violated the duties alleged;

C. Award actual, compensatory, consequential, nominal, restitutionary, and other damages available under the governing law in an amount to be determined at trial;

D. Award restitution, disgorgement, and equitable monetary relief to the extent permitted and not duplicative;

E. Award punitive or exemplary damages to the extent permitted and supported by proof of conscious disregard, oppression, fraud, or malice;

F. Enter appropriate declaratory and injunctive relief, including the security, notice, monitoring, minimization, deletion, and remediation measures described above;

G. Award prejudgment and post-judgment interest;

H. Award reasonable attorneys' fees, litigation expenses, and costs as permitted by law and the common-fund or substantial-benefit doctrines;

I. Retain jurisdiction to administer any classwide relief and enforce compliance; and

J. Grant such other and further relief as the Court deems just and proper.

JURY TRIAL DEMANDED

Plaintiff demands a trial by jury of all claims so triable.

Dated: July 24, 2026

Respectfully Submitted,

/s/ *Margot Cutter*

Margot Cutter (SBN 306789)
mcutter@cutterlaw.com
CUTTER LAW, PC
401 Watt Ave.
Sacramento, CA 95864
Telephone: 916.290.9400
Facsimile: 916.588.9314

Tina Wolfson (SBN 174806)
twolfson@ahdootwolfson.com
Jeff S. Westerman (SBN 94559)
jwesterman@ahdootwolfson.com
Lisa Cintron (SBN 356009)
lcintron@ahdootwolfson.com
AHDOOT & WOLFSON, PC
2600 West Olive Avenue, Suite 500
Burbank, CA 91505
Tel: (310) 474-9111

Nicholas Andrew Hall
Texas Bar No. 24069863
nhall@hallattorneys.com
HALL ATTORNEYS, PC
P.O. Box 1370
Edna, Texas 77957
Telephone: (713) 428-8967

Attorneys for Plaintiff and the Proposed Class

JS 44 (Rev. 04/21)

CIVIL COVER SHEET

The JS 44 civil cover sheet and the information contained herein neither replace nor supplement the filing and service of pleadings or other papers as required by law, except as provided by local rules of court. This form, approved by the Judicial Conference of the United States in September 1974, is required for the use of the Clerk of Court for the purpose of initiating the civil docket sheet. *(SEE INSTRUCTIONS ON NEXT PAGE OF THIS FORM.)*

I. (a) PLAINTIFFS

MAGEN MELISSA VENNOR, individually and on behalf of all others similarly situated

(b) County of Residence of First Listed Plaintiff Edmonton, Canada
(EXCEPT IN U.S. PLAINTIFF CASES)

(c) Attorneys *(Firm Name, Address, and Telephone Number)*

Margot Cutter, Cutter Law P.C.,
401 Watt Ave., Sacramento CA 95864

DEFENDANTS

PAIDWORK LLC

County of Residence of First Listed Defendant Sacramento
(IN U.S. PLAINTIFF CASES ONLY)

NOTE: IN LAND CONDEMNATION CASES, USE THE LOCATION OF THE TRACT OF LAND INVOLVED.

Attorneys *(If Known)*

II. BASIS OF JURISDICTION *(Place an "X" in One Box Only)*

- ☐ 1 U.S. Government Plaintiff
- ☐ 3 Federal Question *(U.S. Government Not a Party)*
- ☐ 2 U.S. Government Defendant
- ☒ 4 Diversity *(Indicate Citizenship of Parties in Item III)*

III. CITIZENSHIP OF PRINCIPAL PARTIES *(Place an "X" in One Box for Plaintiff and One Box for Defendant)*

(For Diversity Cases Only)

	PTF	DEF		PTF	DEF
Citizen of This State	☐ 1	☐ 1	Incorporated *or* Principal Place of Business In This State	☐ 4	☒ 4
Citizen of Another State	☐ 2	☐ 2	Incorporated *and* Principal Place of Business In Another State	☐ 5	☐ 5
Citizen or Subject of a Foreign Country	☒ 3	☐ 3	Foreign Nation	☐ 6	☐ 6

IV. NATURE OF SUIT *(Place an "X" in One Box Only)*

Click here for: Nature of Suit Code Descriptions.

CONTRACT
- ☐ 110 Insurance
- ☐ 120 Marine
- ☐ 130 Miller Act
- ☐ 140 Negotiable Instrument
- ☐ 150 Recovery of Overpayment & Enforcement of Judgment
- ☐ 151 Medicare Act
- ☐ 152 Recovery of Defaulted Student Loans (Excludes Veterans)
- ☐ 153 Recovery of Overpayment of Veteran's Benefits
- ☐ 160 Stockholders' Suits
- ☐ 190 Other Contract
- ☐ 195 Contract Product Liability
- ☐ 196 Franchise

TORTS

PERSONAL INJURY
- ☐ 310 Airplane
- ☐ 315 Airplane Product Liability
- ☐ 320 Assault, Libel & Slander
- ☐ 330 Federal Employers' Liability
- ☐ 340 Marine
- ☐ 345 Marine Product Liability
- ☐ 350 Motor Vehicle
- ☐ 355 Motor Vehicle Product Liability
- ☒ 360 Other Personal Injury
- ☐ 362 Personal Injury - Medical Malpractice

PERSONAL INJURY
- ☐ 365 Personal Injury - Product Liability
- ☐ 367 Health Care/ Pharmaceutical Personal Injury Product Liability
- ☐ 368 Asbestos Personal Injury Product Liability

PERSONAL PROPERTY
- ☐ 370 Other Fraud
- ☐ 371 Truth in Lending
- ☐ 380 Other Personal Property Damage
- ☐ 385 Property Damage Product Liability

FORFEITURE/PENALTY
- ☐ 625 Drug Related Seizure of Property 21 USC 881
- ☐ 690 Other

LABOR
- ☐ 710 Fair Labor Standards Act
- ☐ 720 Labor/Management Relations
- ☐ 740 Railway Labor Act
- ☐ 751 Family and Medical Leave Act
- ☐ 790 Other Labor Litigation
- ☐ 791 Employee Retirement Income Security Act

IMMIGRATION
- ☐ 462 Naturalization Application
- ☐ 465 Other Immigration Actions

BANKRUPTCY
- ☐ 422 Appeal 28 USC 158
- ☐ 423 Withdrawal 28 USC 157

INTELLECTUAL PROPERTY RIGHTS
- ☐ 820 Copyrights
- ☐ 830 Patent
- ☐ 835 Patent - Abbreviated New Drug Application
- ☐ 840 Trademark
- ☐ 880 Defend Trade Secrets Act of 2016

SOCIAL SECURITY
- ☐ 861 HIA (1395ff)
- ☐ 862 Black Lung (923)
- ☐ 863 DIWC/DIWW (405(g))
- ☐ 864 SSID Title XVI
- ☐ 865 RSI (405(g))

FEDERAL TAX SUITS
- ☐ 870 Taxes (U.S. Plaintiff or Defendant)
- ☐ 871 IRS—Third Party 26 USC 7609

OTHER STATUTES
- ☐ 375 False Claims Act
- ☐ 376 Qui Tam (31 USC 3729(a))
- ☐ 400 State Reapportionment
- ☐ 410 Antitrust
- ☐ 430 Banks and Banking
- ☐ 450 Commerce
- ☐ 460 Deportation
- ☐ 470 Racketeer Influenced and Corrupt Organizations
- ☐ 480 Consumer Credit (15 USC 1681 or 1692)
- ☐ 485 Telephone Consumer Protection Act
- ☐ 490 Cable/Sat TV
- ☐ 850 Securities/Commodities/ Exchange
- ☐ 890 Other Statutory Actions
- ☐ 891 Agricultural Acts
- ☐ 893 Environmental Matters
- ☐ 895 Freedom of Information Act
- ☐ 896 Arbitration
- ☐ 899 Administrative Procedure Act/Review or Appeal of Agency Decision
- ☐ 950 Constitutionality of State Statutes

REAL PROPERTY
- ☐ 210 Land Condemnation
- ☐ 220 Foreclosure
- ☐ 230 Rent Lease & Ejectment
- ☐ 240 Torts to Land
- ☐ 245 Tort Product Liability
- ☐ 290 All Other Real Property

CIVIL RIGHTS
- ☐ 440 Other Civil Rights
- ☐ 441 Voting
- ☐ 442 Employment
- ☐ 443 Housing/ Accommodations
- ☐ 445 Amer. w/Disabilities - Employment
- ☐ 446 Amer. w/Disabilities - Other
- ☐ 448 Education

PRISONER PETITIONS

Habeas Corpus:
- ☐ 463 Alien Detainee
- ☐ 510 Motions to Vacate Sentence
- ☐ 530 General
- ☐ 535 Death Penalty

Other:
- ☐ 540 Mandamus & Other
- ☐ 550 Civil Rights
- ☐ 555 Prison Condition
- ☐ 560 Civil Detainee - Conditions of Confinement

V. ORIGIN *(Place an "X" in One Box Only)*

☒ 1 Original Proceeding ☐ 2 Removed from State Court ☐ 3 Remanded from Appellate Court ☐ 4 Reinstated or Reopened ☐ 5 Transferred from Another District *(specify)* ☐ 6 Multidistrict Litigation - Transfer ☐ 8 Multidistrict Litigation - Direct File

VI. CAUSE OF ACTION

Cite the U.S. Civil Statute under which you are filing ***(Do not cite jurisdictional statutes unless diversity)***:
Class Action Fairness Act, 28 U.S.C. § 1332(d)

Brief description of cause:
(1) Negligence (2) Breach of Implied Contract (3) Breach of Confidence (4) Unjust Enrichment related to data breach resulting in disclosure of PII

VII. REQUESTED IN COMPLAINT:

☒ CHECK IF THIS IS A **CLASS ACTION** UNDER RULE 23, F.R.Cv.P.

DEMAND $ 5,000,000

CHECK YES only if demanded in complaint:
JURY DEMAND: ☒ Yes ☐ No

VIII. RELATED CASE(S) IF ANY

(See instructions): JUDGE _____ DOCKET NUMBER _____

DATE July 24, 2026

SIGNATURE OF ATTORNEY OF RECORD /s/ Margot Cutter

FOR OFFICE USE ONLY

RECEIPT # _____ AMOUNT _____ APPLYING IFP _____ JUDGE _____ MAG. JUDGE _____

INSTRUCTIONS FOR ATTORNEYS COMPLETING CIVIL COVER SHEET FORM JS 44

Authority For Civil Cover Sheet

The JS 44 civil cover sheet and the information contained herein neither replaces nor supplements the filings and service of pleading or other papers as required by law, except as provided by local rules of court. This form, approved by the Judicial Conference of the United States in September 1974, is required for the use of the Clerk of Court for the purpose of initiating the civil docket sheet. Consequently, a civil cover sheet is submitted to the Clerk of Court for each civil complaint filed. The attorney filing a case should complete the form as follows:

I.(a) Plaintiffs-Defendants. Enter names (last, first, middle initial) of plaintiff and defendant. If the plaintiff or defendant is a government agency, use only the full name or standard abbreviations. If the plaintiff or defendant is an official within a government agency, identify first the agency and then the official, giving both name and title.

(b) County of Residence. For each civil case filed, except U.S. plaintiff cases, enter the name of the county where the first listed plaintiff resides at the time of filing. In U.S. plaintiff cases, enter the name of the county in which the first listed defendant resides at the time of filing. (NOTE: In land condemnation cases, the county of residence of the "defendant" is the location of the tract of land involved.)

(c) Attorneys. Enter the firm name, address, telephone number, and attorney of record. If there are several attorneys, list them on an attachment, noting in this section "(see attachment)".

II. Jurisdiction. The basis of jurisdiction is set forth under Rule 8(a), F.R.Cv.P., which requires that jurisdictions be shown in pleadings. Place an "X" in one of the boxes. If there is more than one basis of jurisdiction, precedence is given in the order shown below.
United States plaintiff. (1) Jurisdiction based on 28 U.S.C. 1345 and 1348. Suits by agencies and officers of the United States are included here.
United States defendant. (2) When the plaintiff is suing the United States, its officers or agencies, place an "X" in this box.
Federal question. (3) This refers to suits under 28 U.S.C. 1331, where jurisdiction arises under the Constitution of the United States, an amendment to the Constitution, an act of Congress or a treaty of the United States. In cases where the U.S. is a party, the U.S. plaintiff or defendant code takes precedence, and box 1 or 2 should be marked.
Diversity of citizenship. (4) This refers to suits under 28 U.S.C. 1332, where parties are citizens of different states. When Box 4 is checked, the citizenship of the different parties must be checked. (See Section III below**; NOTE: federal question actions take precedence over diversity cases.**)

III. Residence (citizenship) of Principal Parties. This section of the JS 44 is to be completed if diversity of citizenship was indicated above. Mark this section for each principal party.

IV. Nature of Suit. Place an "X" in the appropriate box. If there are multiple nature of suit codes associated with the case, pick the nature of suit code that is most applicable. Click here for: Nature of Suit Code Descriptions.

V. Origin. Place an "X" in one of the seven boxes.
Original Proceedings. (1) Cases which originate in the United States district courts.
Removed from State Court. (2) Proceedings initiated in state courts may be removed to the district courts under Title 28 U.S.C., Section 1441.
Remanded from Appellate Court. (3) Check this box for cases remanded to the district court for further action. Use the date of remand as the filing date.
Reinstated or Reopened. (4) Check this box for cases reinstated or reopened in the district court. Use the reopening date as the filing date.
Transferred from Another District. (5) For cases transferred under Title 28 U.S.C. Section 1404(a). Do not use this for within district transfers or multidistrict litigation transfers.
Multidistrict Litigation – Transfer. (6) Check this box when a multidistrict case is transferred into the district under authority of Title 28 U.S.C. Section 1407.
Multidistrict Litigation – Direct File. (8) Check this box when a multidistrict case is filed in the same district as the Master MDL docket.
PLEASE NOTE THAT THERE IS NOT AN ORIGIN CODE 7. Origin Code 7 was used for historical records and is no longer relevant due to changes in statute.

VI. Cause of Action. Report the civil statute directly related to the cause of action and give a brief description of the cause. **Do not cite jurisdictional statutes unless diversity.** Example: U.S. Civil Statute: 47 USC 553 Brief Description: Unauthorized reception of cable service.

VII. Requested in Complaint. Class Action. Place an "X" in this box if you are filing a class action under Rule 23, F.R.Cv.P.
Demand. In this space enter the actual dollar amount being demanded or indicate other demand, such as a preliminary injunction.
Jury Demand. Check the appropriate box to indicate whether or not a jury is being demanded.

VIII. Related Cases. This section of the JS 44 is used to reference related pending cases, if any. If there are related pending cases, insert the docket numbers and the corresponding judge names for such cases.

Date and Attorney Signature. Date and sign the civil cover sheet.