

**UNITED STATES DISTRICT COURT
EASTERN DISTRICT OF KENTUCKY
LONDON DIVISION**

JONATHAN PHELPS, individually and on behalf of all others similarly situated	:	Judge:
	:	Magistrate:
	:	
Plaintiff,	:	[FORMERLY CIRCUIT COURT CASE NO. 22-CI-00328]
v.	:	
	:	<u>NOTICE OF REMOVAL</u>
TOYOTETSU NORTH AMERICA	:	
	:	<u>(Filed Electronically)</u>
Defendant.	:	

NOTICE OF REMOVAL

Pursuant to 28 U.S.C. §§ 1332, 1441, and 1446, Defendant Toyotetsu North America (“Toyotetsu”), provides this Notice of Removal of this action to the United States District Court for the Eastern District of Kentucky, and respectfully represents:

1. On or about April 14, 2022, Jonathan Phelps (“Plaintiff”) commenced a class action suit in the Pulaski Circuit Court, Commonwealth of Kentucky, entitled *Phelps v. Toyotetsu North America*, Civil Action No. 22-CI-00328 (“Action”).
2. Plaintiff purports to bring the Action on behalf of himself and all others similarly situated (i.e., a putative class). Compl. *passim*.
3. Plaintiff claims he and the putative class suffered various forms of injury and damages because of a data security incident whereby unauthorized third parties launched a cyberattack against Defendant’s data network. *See generally* Compl. ¶¶ 1-2.
4. The Complaint asserts these counts: Negligence (Count I), Breach of Implied Contract (Count II), Unjust Enrichment (Count III), and Negligence *per se* (Count IV).

5. Service of process was made on Toyotetsu on April 15, 2022, through its registered agent, Gregory Cowan. *See* Kentucky Clerk of Courts Dkt. Exhibit A.

6. Pursuant to 28 U.S.C. § 1441, Toyotetsu seeks removal of the Action from Pulaski Circuit Court to the United States District Court for the Eastern District of Kentucky. *See also* 28 U.S.C. § 97. This Court has original jurisdiction pursuant to the Class Action Fairness Act (28 U.S.C. § 1332(d)) (“CAFA”) because, as Plaintiff admits (Compl. ¶ 13):

The amount in controversy exceeds the sum of \$5,000,000 exclusive of interest and costs, there are more than 100 putative class members, and minimal diversity exists because many putative class members are citizens of a different state than Defendant.

7. Plaintiff also agrees federal jurisdiction is appropriate under 28 U.S.C. § 1367(a) “because all claims alleged herein form part of the same case or controversy.” Compl. ¶ 13.

JURISDICTION UNDER CAFA

8. This Court has original jurisdiction over the Action pursuant to CAFA because: (i) minimum diversity is admitted, (ii) the number of putative class members exceeds 100, and (iii) the amount in controversy exceeds \$5,000,000. 28 U.S.C. §§ 1332(d)(2), (d)(5).

9.. Again, Plaintiff readily concedes and rightly avers facts demonstrating all three requirements for CAFA jurisdiction are present. Compl. ¶ 13.

10. Concerning minimum diversity, Defendant is a Kentucky corporation with its principal place of business in Kentucky. Compl. ¶ 14. Plaintiff avers “many putative class members are citizens of a different state than Defendant.” Compl. ¶ 13. This is all that is needed for CAFA diversity. 28 U.S.C. §§ 1332(d)(2)(A) (prong met when “any member of a class of plaintiffs is a citizen of a State different from any defendant”).

11. Concerning class size, Plaintiff contends the cyberattack affected “approximately 12,450 individuals,” and on that basis, Plaintiff asserts the Action meets the numerosity

requirement for class status. Compl. ¶ 86. The number of putative class members exceeds, by thousands, the 100-class member threshold for CAFA jurisdiction. 28 U.S.C. § 1332 (d)(5)(B).

12. Concerning the amount in controversy, Plaintiff states it exceeds, excluding interest and costs, \$5,000,000. Compl. ¶ 13. And in support, Plaintiff contends he and the putative class, more than 12,000 supposed members, suffered an array of purported damages, including amounts associated with “identity theft, loss of value of their PII, out-of-pocket expenses and the value of their time reasonably incurred,” as well as “punitive damages” and damages arising from contractual breach. Compl. ¶¶ 2, 110, 124. *See id.* ¶ 125 (class is “entitled to compensatory and consequential damages”).¹ The amount in controversy satisfies CAFA. 28 U.S.C. § 1332(d)(2). *See also Dart Cherokee Basin Operating Co. v. Owens*, 574 U.S. 81, 89 (2014) (finding “only a plausible allegation” of the amount of controversy is required in noticing removal).

DEFENDANT HAS MEET ALL OTHER REMOVAL REQUIREMENTS

13. In accordance with 28 U.S.C. § 1446(a), copies of all process, pleadings, and orders served on Toyotetsu in the Action are attached at Exhibit A and B, including the Complaint.

14. As required by 28 U.S.C. § 1446(b), this Notice of Removal is filed within thirty (30) days after service of a summons or the Complaint on Defendant.

15. Consistent with 28 U.S.C. § 1446(d), a true and correct copy of this Notice of Removal promptly will be filed with the Clerk of Court for the Pulaski Circuit Court, Commonwealth of Kentucky, and written notice shall be given promptly to Plaintiff, the adverse party.

16. Venue is proper for purposes of removal in this Court because Pulaski County,

¹ *See also Hayes v. Equitable Energy Res. Co.*, 266 F.3d 560, 572 (6th Cir. 2001) (“When determining the jurisdictional amount in controversy in diversity cases, punitive damages must be considered” (citation omitted)).

Kentucky is found within the Eastern District of Kentucky. *See* 28 U.S.C. § 97. This federal judicial district embraces the place, the Pulaski Circuit Court, where the Action is pending. 28 U.S.C. §§ 1441(a) and 1446(a).

17. Through this notice, Defendant reserves all defenses, objections, and exceptions to the Action, including but not limited to objections to service and personal jurisdiction. Defendant also does not intend and denies any admission of law, liability, or damages in connection with the Action and reserves all of its rights to defend, including through appropriate motion, defenses, pleas, and challenges to contentions of fact.

CONCLUSION

Having provided a sufficient “short and plain statement of the grounds for removal” and having met all other conditions and procedures for removal to federal district court, this Action should be removed from the Pulaski Circuit Court to the United States District Court for the Eastern District of Kentucky.

Dated: May 13, 2022

Respectfully,

/s/ R. Morgan Salisbury
Judd R. Uhl (89578)
R. Morgan Salisbury (94922)
Lewis Brisbois Bisgaard & Smith, LLP
250 E. Fifth Street, Suite 2000
Cincinnati, OH 45202
judd.uhl@lewisbrisbois.com
morgan.salisbury@lewisbrisbois.com
Phone: (513) 808-9911
Attorneys for Toyotetsu North America

CERTIFICATE OF SERVICE

I hereby certify that on May 13, 2022, I served a copy of the foregoing via electronic filing in the ECF system.

/s/ R. Morgan Salisbury
Judd R. Uhl (89578)
R. Morgan Salisbury (94922)

JS 44 (Rev. 10/20)

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.)

<p>I. (a) PLAINTIFFS Jonathan Phelps, individually and on behalf of all others similarly situated</p> <p>(b) County of Residence of First Listed Plaintiff <u>Kentucky (alleged)</u> <i>(EXCEPT IN U.S. PLAINTIFF CASES)</i></p> <p>(c) Attorneys (Firm Name, Address, and Telephone Number) Terence R. Coates, 3825 Edwards Road, Suite 650, Cincinnati, OH 45209, 513.651.3700</p>	<p>DEFENDANTS Toyotetsu North America</p> <p>County of Residence of First Listed Defendant <u>Pulaski County, KY</u> <i>(IN U.S. PLAINTIFF CASES ONLY)</i></p> <p>NOTE: IN LAND CONDEMNATION CASES, USE THE LOCATION OF THE TRACT OF LAND INVOLVED.</p> <p>Attorneys (If Known) R. Morgan Salisbury, 250 East Fifth St., Suite 2000, Cincinnati, OH 45202, 513.808.9912</p>
---	--

<p>II. BASIS OF JURISDICTION (Place an "X" in One Box Only)</p> <p><input type="checkbox"/> 1 U.S. Government Plaintiff</p> <p><input type="checkbox"/> 2 U.S. Government Defendant</p> <p><input type="checkbox"/> 3 Federal Question (U.S. Government Not a Party)</p> <p><input checked="" type="checkbox"/> 4 Diversity (Indicate Citizenship of Parties in Item III)</p>	<p>III. CITIZENSHIP OF PRINCIPAL PARTIES (Place an "X" in One Box for Plaintiff and One Box for Defendant)</p> <table border="1" style="width:100%; border-collapse: collapse;"> <tr> <td></td> <td>PTF</td> <td>DEF</td> <td></td> <td>PTF</td> <td>DEF</td> </tr> <tr> <td>Citizen of This State</td> <td><input checked="" type="checkbox"/> 1</td> <td><input type="checkbox"/> 1</td> <td>Incorporated or Principal Place of Business In This State</td> <td><input type="checkbox"/> 4</td> <td><input checked="" type="checkbox"/> 4</td> </tr> <tr> <td>Citizen of Another State</td> <td><input type="checkbox"/> 2</td> <td><input type="checkbox"/> 2</td> <td>Incorporated and Principal Place of Business In Another State</td> <td><input type="checkbox"/> 5</td> <td><input type="checkbox"/> 5</td> </tr> <tr> <td>Citizen or Subject of a Foreign Country</td> <td><input type="checkbox"/> 3</td> <td><input type="checkbox"/> 3</td> <td>Foreign Nation</td> <td><input type="checkbox"/> 6</td> <td><input type="checkbox"/> 6</td> </tr> </table>		PTF	DEF		PTF	DEF	Citizen of This State	<input checked="" type="checkbox"/> 1	<input type="checkbox"/> 1	Incorporated or Principal Place of Business In This State	<input type="checkbox"/> 4	<input checked="" type="checkbox"/> 4	Citizen of Another State	<input type="checkbox"/> 2	<input type="checkbox"/> 2	Incorporated and Principal Place of Business In Another State	<input type="checkbox"/> 5	<input type="checkbox"/> 5	Citizen or Subject of a Foreign Country	<input type="checkbox"/> 3	<input type="checkbox"/> 3	Foreign Nation	<input type="checkbox"/> 6	<input type="checkbox"/> 6
	PTF	DEF		PTF	DEF																				
Citizen of This State	<input checked="" type="checkbox"/> 1	<input type="checkbox"/> 1	Incorporated or Principal Place of Business In This State	<input type="checkbox"/> 4	<input checked="" type="checkbox"/> 4																				
Citizen of Another State	<input type="checkbox"/> 2	<input type="checkbox"/> 2	Incorporated and Principal Place of Business In Another State	<input type="checkbox"/> 5	<input type="checkbox"/> 5																				
Citizen or Subject of a Foreign Country	<input type="checkbox"/> 3	<input type="checkbox"/> 3	Foreign Nation	<input type="checkbox"/> 6	<input type="checkbox"/> 6																				

IV. NATURE OF SUIT (Place an "X" in One Box Only) Click here for: [Nature of Suit Code Descriptions.](#)

CONTRACT	TORTS	FORFEITURE/PENALTY	BANKRUPTCY	OTHER STATUTES	
<input type="checkbox"/> 110 Insurance <input type="checkbox"/> 120 Marine <input type="checkbox"/> 130 Miller Act <input type="checkbox"/> 140 Negotiable Instrument <input type="checkbox"/> 150 Recovery of Overpayment & Enforcement of Judgment <input type="checkbox"/> 151 Medicare Act <input type="checkbox"/> 152 Recovery of Defaulted Student Loans (Excludes Veterans) <input type="checkbox"/> 153 Recovery of Overpayment of Veteran's Benefits <input type="checkbox"/> 160 Stockholders' Suits <input type="checkbox"/> 190 Other Contract <input type="checkbox"/> 195 Contract Product Liability <input type="checkbox"/> 196 Franchise	<p>PERSONAL INJURY</p> <input type="checkbox"/> 310 Airplane <input type="checkbox"/> 315 Airplane Product Liability <input type="checkbox"/> 320 Assault, Libel & Slander <input type="checkbox"/> 330 Federal Employers' Liability <input type="checkbox"/> 340 Marine <input type="checkbox"/> 345 Marine Product Liability <input type="checkbox"/> 350 Motor Vehicle <input type="checkbox"/> 355 Motor Vehicle Product Liability <input checked="" type="checkbox"/> 360 Other Personal Injury <input type="checkbox"/> 362 Personal Injury - Medical Malpractice	<p>PERSONAL INJURY</p> <input type="checkbox"/> 365 Personal Injury - Product Liability <input type="checkbox"/> 367 Health Care/Pharmaceutical Personal Injury Product Liability <input type="checkbox"/> 368 Asbestos Personal Injury Product Liability <p>PERSONAL PROPERTY</p> <input type="checkbox"/> 370 Other Fraud <input type="checkbox"/> 371 Truth in Lending <input type="checkbox"/> 380 Other Personal Property Damage <input type="checkbox"/> 385 Property Damage Product Liability	<input type="checkbox"/> 625 Drug Related Seizure of Property 21 USC 881 <input type="checkbox"/> 690 Other <p>LABOR</p> <input type="checkbox"/> 710 Fair Labor Standards Act <input type="checkbox"/> 720 Labor/Management Relations <input type="checkbox"/> 740 Railway Labor Act <input type="checkbox"/> 751 Family and Medical Leave Act <input type="checkbox"/> 790 Other Labor Litigation <input type="checkbox"/> 791 Employee Retirement Income Security Act <p>IMMIGRATION</p> <input type="checkbox"/> 462 Naturalization Application <input type="checkbox"/> 465 Other Immigration Actions	<input type="checkbox"/> 422 Appeal 28 USC 158 <input type="checkbox"/> 423 Withdrawal 28 USC 157 <p>PROPERTY RIGHTS</p> <input type="checkbox"/> 820 Copyrights <input type="checkbox"/> 830 Patent <input type="checkbox"/> 835 Patent - Abbreviated New Drug Application <input type="checkbox"/> 840 Trademark <input type="checkbox"/> 880 Defend Trade Secrets Act of 2016 <p>SOCIAL SECURITY</p> <input type="checkbox"/> 861 HIA (1395ff) <input type="checkbox"/> 862 Black Lung (923) <input type="checkbox"/> 863 DIWC/DIWW (405(g)) <input type="checkbox"/> 864 SSID Title XVI <input type="checkbox"/> 865 RSI (405(g)) <p>FEDERAL TAX SUITS</p> <input type="checkbox"/> 870 Taxes (U.S. Plaintiff or Defendant) <input type="checkbox"/> 871 IRS—Third Party 26 USC 7609	<input type="checkbox"/> 375 False Claims Act <input type="checkbox"/> 376 Qui Tam (31 USC 3729(a)) <input type="checkbox"/> 400 State Reapportionment <input type="checkbox"/> 410 Antitrust <input type="checkbox"/> 430 Banks and Banking <input type="checkbox"/> 450 Commerce <input type="checkbox"/> 460 Deportation <input type="checkbox"/> 470 Racketeer Influenced and Corrupt Organizations <input type="checkbox"/> 480 Consumer Credit (15 USC 1681 or 1692) <input type="checkbox"/> 485 Telephone Consumer Protection Act <input type="checkbox"/> 490 Cable/Sat TV <input type="checkbox"/> 850 Securities/Commodities/Exchange <input type="checkbox"/> 890 Other Statutory Actions <input type="checkbox"/> 891 Agricultural Acts <input type="checkbox"/> 893 Environmental Matters <input type="checkbox"/> 895 Freedom of Information Act <input type="checkbox"/> 896 Arbitration <input type="checkbox"/> 899 Administrative Procedure Act/Review or Appeal of Agency Decision <input type="checkbox"/> 950 Constitutionality of State Statutes
<p>REAL PROPERTY</p> <input type="checkbox"/> 210 Land Condemnation <input type="checkbox"/> 220 Foreclosure <input type="checkbox"/> 230 Rent Lease & Ejectment <input type="checkbox"/> 240 Torts to Land <input type="checkbox"/> 245 Tort Product Liability <input type="checkbox"/> 290 All Other Real Property	<p>CIVIL RIGHTS</p> <input type="checkbox"/> 440 Other Civil Rights <input type="checkbox"/> 441 Voting <input type="checkbox"/> 442 Employment <input type="checkbox"/> 443 Housing/Accommodations <input type="checkbox"/> 445 Amer. w/Disabilities - Employment <input type="checkbox"/> 446 Amer. w/Disabilities - Other <input type="checkbox"/> 448 Education	<p>PRISONER PETITIONS</p> <p>Habeas Corpus:</p> <input type="checkbox"/> 463 Alien Detainee <input type="checkbox"/> 510 Motions to Vacate Sentence <input type="checkbox"/> 530 General <input type="checkbox"/> 535 Death Penalty <p>Other:</p> <input type="checkbox"/> 540 Mandamus & Other <input type="checkbox"/> 550 Civil Rights <input type="checkbox"/> 555 Prison Condition <input type="checkbox"/> 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):
28 U.S.C. 1332(d); 28 U.S.C. 1441; 28 U.S.C. 1446

Brief description of cause:
Class action related to data security incident alleging common law negligence, negligence per se, unjust enrichment, and breach of implied contract

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: May 13, 2022 SIGNATURE OF ATTORNEY OF RECORD: R. Morgan Salisbury

FOR OFFICE USE ONLY

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

EXHIBIT A



22-CI-00328

PHELPS, JONATHAN VS. TOYOTETSU NORTH AMERICA

PULASKI CIRCUIT COURT

Filed on **04/14/2022** as **TORT - OTHER** with **HON. JOHN G. PRATHER JR.**

*** NOT AN OFFICIAL COURT RECORD ***

Case Memo 22-CI-00328

TORT OTHER

Parties 22-CI-00328

PHELPS, JONATHAN as **PLAINTIFF / PETITIONER**

TOYOTETSU NORTH AMERICA as **DEFENDANT / RESPONDENT**

Memo

Registered Agent of Service exists.

Summons

CIVIL SUMMONS issued on **04/14/2022** served / recalled on **04/15/2022** by way of **RETURNED TO ATTORNEY/PETITIONER**

UHL, JUDD RICHARDS as **ATTORNEY FOR DEFENDANT**

Address

LEWIS BRISBOIS BISGAARD & SMITH, LLP
250 E. FIFTH STREET, SUITE 2000
CINCINNATI OH 45202

UHL, JUDD RICHARDS as **ATTORNEY FOR DEFENDANT**

Address

LEWIS BRISBOIS BISGAARD & SMITH, LLP
250 E. FIFTH STREET, SUITE 2000
CINCINNATI OH 45202

VENTERS, JOSEPH BRAND as **ATTORNEY FOR PLAINTIFF**

Address

VENTERS LAW OFFICE
P.O. BOX 1749
SOMERSET KY 42502

COWAN, GREGORY A. as **REGISTERED AGENT OF SERVICE**

Memo

Related party is TOYOTETSU NORTH AMERICA

Address

100 PIN OAK DRIVE
SOMERSET KY 42503

Documents 22-CI-00328

COMPLAINT / PETITION filed on **04/14/2022**

CIVIL CASE COVER SHEET filed on **04/14/2022**

ENTRY OF APPEARANCE filed on **05/04/2022**

TENDERED DOCUMENT filed on **05/04/2022**

ORDER - AGREED entered on **05/06/2022**

HAVE UP TO MAY 31 2022 TO FILE A RESPONSIVE PLEADING TO PLAINTIFFS COMPLAINT

Images	22-CI-00328
COMPLAINT / PETITION filed on 04/14/2022 Page(s): 33	
SUMMONS filed on 04/14/2022 Page(s): 1	
CIVIL CASE COVER SHEET filed on 04/14/2022 Page(s): 1	
COURTESY FINANCIAL TRANSACTION REPORT filed on 04/14/2022 Page(s): 1	
ENTRY OF APPEARANCE filed on 05/04/2022 Page(s): 2	
TENDERED DOCUMENT filed on 05/04/2022 Page(s): 2	

**** End of Case Number : 22-CI-00328 ****

EXHIBIT B

AOC-104 Doc. Code: CCCS
Rev. 9-21
Page 1 of 1
Commonwealth of Kentucky
Court of Justice www.kycourts.gov



CIVIL CASE COVER SHEET

Court: Circuit
County: Pulaski
Division:

PLAINTIFF/PETITIONER OR IN RE/IN THE INTEREST OF:
JONATHAN PHELPS, individually and on behalf of all others similarly situated

DEFENDANT/RESPONDENT, if applicable:
TOYOTETSU NORTH AMERICA

Check here if YOU DO NOT HAVE AN ATTORNEY and are REPRESENTING YOURSELF (a Self-Represented [Pro Se] Litigant)

Nature of the Case: Place a "X" to the left of the ONE case category that most accurately describes your PRIMARY CASE. If you are making more than one type of claim, check the one that you consider most important.

DOMESTIC RELATIONS

- Dissolution/Divorce with Children (DISSOC)
- Dissolution/Divorce without Children (DISSO)
- Paternity (PA)
- Custody (CUSTO)
- Child Support IV-D (SUPIV)
- Child Support Private Non IV-D (SUPPRI)
- URESA/UIFSA (UR)
- Visitation/Parenting Time (VISIT)
- Voluntary Termination of Parental Rights (VTPR)
- Involuntary Termination of Parental Rights (ITPR)
- Adoption (ADPT)
- Other: (DFOTH)

TORT (Injury)

- Automobile (AUTO)
- Intentional (INTENT)
- Malpractice-Medical (MDML)
- Malpractice-Other (MLOTH)
- Premises Liability (PREM)
- Product Liability (PROD)
- Property Damage (PD)
- Slander/Libel/Defamation (SLAND)
- Other: (PIOTH)

CONSUMER

- Seller Consumer Goods (DEBTG)
- Seller Consumer Services (DEBTS)
- Buyer Consumer Goods (BUYERG)
- Buyer Consumer Services (BUYERS)
- Credit Card Debt (CREDIT)
- Fraud (FRAUD)
- Other: (COOTH)

APPEALS

- Appeal from Administrative Agency (AB)
- Appeal from District Court (XI)
- Other: (OTH)

PROBATE / ESTATE

- Guardianship-Adult (GCADLT)
- Guardianship-Juvenile (GCJUV)
- Adult Conservatorship - Trusteeship (CONVA)
- Juvenile Conservatorship - Trusteeship (CONVJ)
- Probate-Testate (with a will) (PBTEST)
- Probate-Intestate (without a will) (PBINT)
- Petition to Dispense with Administration (PBDIS)
- Name Change (NC)
- Will Contest (WC)
- Other: (PBOH)

REAL PROPERTY

- Abandoned and Blighted Property Conservatorship (PC)
- Property Rights (PR)
- Condemnation (DOMAIN)
- Forcible Detainer - Eviction (FD)
- Forcible Entry (FENTRY)
- Foreclosure (FCL)
- Other: (COOTH)

MISC CIVIL

- Constitutional Challenge (CCHAL)
- Habeas Corpus (HABEAS)
- Non-Domestic Relations Restraining Order (IP)
- Tax (TAX)
- Writs (WRITS)
- Other: (OTH)

EMPLOYMENT

- Employment-Discrimination (DSCR)
- Employment-Other (DISPU)

BUSINESS / COMMERCIAL

- Business Tort (BCPI)
- Statutory Action (BCSA)
- Business Contract Dispute (BCCO)
- Other: (BCOTH)

**COMMONWEALTH OF KENTUCKY
28TH JUDICIAL CIRCUIT
PULASKI CIRCUIT COURT
CIVIL ACTION NO. 22-CI-_____**

JONATHAN PHELPS, individually and
on behalf of all others similarly situated

PLAINTIFF

vs.

TOYOTETSU NORTH AMERICA
Serve By: Constable
Registered Agent: Gregroy A. Cowan
100 Pin Oak Drive
Somerset, Kentucky 42503

DEFENDANT

**CLASS ACTION CIVIL COMPLAINT

Plaintiff JONATHAN PHELPS (“Plaintiff”) brings this Class Action Complaint against TOYOTETSU NORTH AMERICA (“Defendant” or “Toyotetsu”), in his individual capacity and on behalf of all others similarly situated, and alleges, upon personal knowledge as to his own actions and his counsels’ investigations, and upon information and belief as to all other matters, as follows:

I. INTRODUCTION

1. This class action arises out of the recent data breach (“Data Breach”) involving Defendant Toyotetsu, a for-profit manufacturer of car components located in Somerset, Kentucky
2. Toyotetsu failed to reasonably secure, monitor, and maintain Personally Identifiable Information (“PII”) provided by employees and consumers, including, without limitation, full names, addresses, and Social Security numbers of individuals stored on its private network. As a result, Plaintiff and other impacted individuals suffered present injury and damages in the form of identity theft, loss of value of their PII, out-of-pocket expenses and the value of their time reasonably incurred to remedy or mitigate the effects of the unauthorized access, exfiltration, and

subsequent criminal misuse of their sensitive and highly personal information.

3. Moreover, after learning of the Data Breach, Defendant waited nearly two months to notify Plaintiff and Class Members of the Data Breach and/or inform them that their PII was compromised. During this time, Plaintiff and Class Members were unaware that their sensitive PII had been compromised, and that they were, and continue to be, at significant risk of identity theft and various other forms of personal, social, and financial harm.

4. By obtaining, collecting, using, and deriving a benefit from the PII of Plaintiff and Class Members, Defendant assumed legal and equitable duties to those individuals to protect and safeguard that information from unauthorized access and intrusion. Defendant's conduct in breaching these duties amounts to negligence and/or recklessness and violates federal and state statutes.

5. Plaintiff brings this action on behalf of all persons whose PII was compromised as a result of Defendant's failure to take reasonable steps to protect the PII of Plaintiff and Class Members and warn Plaintiff and Class Members of Defendant's inadequate information security practices. Defendant disregarded the rights of Plaintiff and Class Members by knowingly failing to implement and maintain adequate and reasonable measures to ensure that the PII of Plaintiff and Class Members was safeguarded, failing to take available steps to prevent an unauthorized disclosure of data, and failing to follow applicable, required, and appropriate protocols, policies, and procedures regarding the encryption of data, even for internal use.

6. As a direct and proximate result of Defendant's data security failures and the Data Breach, the PII of Plaintiff and Class Members was compromised through disclosure to an unknown and unauthorized third party, and Plaintiff and Class Members have suffered actual, present, concrete injuries. These injuries include: (i) the current and imminent risk of fraud and

identity theft (ii) lost or diminished value of PII ; (iii) out-of-pocket expenses associated with the prevention, detection, and recovery from identity theft, tax fraud, and/or unauthorized use of their PII; (iv) lost opportunity costs associated with attempting to mitigate the actual consequences of the Data Breach, including but not limited to lost time; and (v) the continued and certainly increased risk to their PII, which: (a) remains unencrypted and available for unauthorized third parties to access and abuse; and (b) may remain backed up in Defendant’s possession and is subject to further unauthorized disclosures so long as Defendant fails to undertake appropriate and adequate measures to protect the PII; (vi) the invasion of privacy; (vii) the compromise, disclosure, theft, and unauthorized use of Plaintiff’s and the Class Members’ PII; and (viii) emotional distress, fear, anxiety, nuisance and annoyance related to the theft and compromise of their PII.

7. Plaintiff and Class Members seek to remedy these harms and prevent any future data compromise on behalf of themselves and all similarly situated persons whose personal data was compromised and stolen as a result of the Data Breach and remains at risk due to inadequate data security.

8. Plaintiff and Class Members have a continuing interest in ensuring that their information is and remains safe, and they should be entitled to injunctive and other equitable relief.

II. PARTIES

Plaintiff Jonathan Phelps

9. Plaintiff Jonathan Phelps is, and at all times relevant has been, a resident and citizen of Kentucky, where he intends to remain. Plaintiff received a “Notice of Security” letter, dated November 24, 2021, on or about that date. The letter notified Plaintiff that on October 7, 2021, Toyotetsu identified unusual activity on its network and that “certain files containing personal

information may have been accessed or acquired without authorization.”¹ The type of data at issue included full names, addresses, and Social Security numbers.² The letter further advised that Plaintiff that he could participate in credit monitoring services detecting suspicious activity.

10. Defendant obtained and continues to maintain Plaintiff’s and Class Members’ PII and has a continuing legal duty and obligation to protect that sensitive information from unauthorized access and disclosure. Defendant required the PII from Plaintiff. Plaintiff, however, would not have entrusted his PII to Defendant had he known that it would fail to maintain adequate data security. Plaintiff’s PII was compromised and disclosed as a result of the Data Breach.

Defendant Toyotetsu North America

11. Defendant Toyotetsu is Kentucky corporation headquartered in and with a principal office location of 100 Pin Oak Drive, Somerset, Kentucky 42503. Toyotetsu is a manufacturer of car components that was established in Somerset, KY in 1995, and began production in 1997. Toyotetsu’s customers include Toyota Motor Manufacturing Kentucky, Nissan, and Subaru.

12. All of Plaintiff’s claims stated herein are asserted against Defendant and any of its owners, predecessors, successors, subsidiaries, agents and/or assigns.

III. JURISDICTION AND VENUE

13. This Court has subject matter jurisdiction pursuant to the Class Action Fairness Act of 2005 (“CAFA”), 28 U.S.C. § 1332(d). The amount in controversy exceeds the sum of \$5,000,000 exclusive of interest and costs, there are more than 100 putative class members, and minimal diversity exists because many putative class members are citizens of a different state than

¹ <https://apps.web.maine.gov/online/aeviewer/ME/40/275fde84-6559-4ed0-9ba4-a7a4a3d75dee.shtml>

² *Id.*

Defendant. This Court also has supplemental jurisdiction pursuant to 28 U.S.C. § 1367(a) because all claims alleged herein form part of the same case or controversy.

14. This Court has personal jurisdiction over Toyotetsu because it is headquartered in and maintains its principal place of business in this county. Toyotetsu is authorized to and regularly conducts business in Kentucky.

15. This Court has jurisdiction over the parties and over the subject matter by virtue of KRS Chapter 338; KRS 446.070; KRS 411.184(2); and because the amount in dispute exceeds the minimum dollar amount needed to establish jurisdiction in this Court.

16. This Court is the proper place of venue pursuant to KRS Chapter 338; KRS 446.070; KRS 411.184(2); and because all the unlawful acts and/or unlawful omissions complained herein all occurred in Somerset, Kentucky.

IV. FACTUAL ALLEGATIONS

Background

17. Defendant is a manufacturer of car components that was established in Somerset, KY with customers that include Toyota Motor Manufacturing Kentucky, Nissan, and Subaru.

18. Plaintiff and Class Members were customers and/or employees of Defendant whose PII was required to be provided, and was in fact provided, to Defendant in conjunction with manufacturing of car components or during the course of their employment with Defendant. Plaintiff's and Class Members' PII were required to fill out various forms, including without limitation employment paperwork and applications, tax documents, various authorizations, other form documents associated with the manufacturing of car components, and employment documentation.

19. Plaintiff and Class Members relied on the sophistication of Defendant and its network to keep their PII confidential and securely maintained, to use this information for business and/or employment purposes only, and to make only authorized disclosures of this information. Plaintiff and Class Members demand security to safeguard their PII.

20. Defendant required the submission of and voluntarily accepted the PII as part of its business and had a duty to adopt reasonable measures to protect the PII of Plaintiff and Class Members from involuntary disclosure to third parties. Toyotetsu has a legal duty to keep employee and consumer PII safe and confidential.

21. The information held by Defendant in its computer systems and networks included the PII of Plaintiff and Class Members.

22. Defendant derived a substantial economic benefit from collecting Plaintiff's and Class Members' PII.

23. By obtaining, collecting, using, and deriving a benefit from Plaintiff's and Class Members' PII, Toyotetsu assumed legal and equitable duties and knew or should have known that it was responsible for protecting Plaintiff's and Class Members' PII from disclosure.

24. Plaintiff and the Class Members have taken reasonable steps to maintain the confidentiality of their PII.

The Data Breach

25. "On October 7, 2021, Toyotetsu detected unusual network activity impacting certain systems."³

26. According to Defendant, Toyotetsu alleges that it conducted "an investigation to determine what happened and whether any personal information was accessed or acquired without

³ <https://apps.web.maine.gov/online/aeviewer/ME/40/275fde84-6559-4ed0-9ba4-a7a4a3d75dee.shtml>

authorization as a result. Through the investigation, Toyotetsu learned that certain files containing personal information may have been accessed or acquired without authorization.”⁴

27. To date, Toyotetsu has not revealed when the unauthorized actor first gained access to a portion of Defendant’s network, nor has it revealed the mechanism by which the unauthorized actor first gained access to Defendant’s network.

28. Upon information and belief, the unauthorized actor gained access to Toyotetsu’s network well in advance of the October 7, 2021 date that the intrusion was first discovered by Toyotetsu, meaning that the unauthorized actor had unfettered and undetected access to Defendant’s networks for a considerable period of time prior to Toyotetsu becoming aware of the unauthorized access to its computer systems and network.

29. After Toyotetsu initially discovery the unauthorized access to its systems, Toyotetsu commissioned computer forensic specialists to conduct an investigation to determine the nature and scope of the event.

30. The investigation commissioned by Toyotetsu did not conclude until November 16, 2021, and notice was not sent to victims of the data breach at least a week after that.⁵ Thus, the victims of this Data Breach, including Plaintiff and Class Members, were not sent notice of this Data Breach until approximately eight weeks after Toyotetsu first knew about this Data Breach.

31. Defendant acknowledged that “certain files containing personal information may have been accessed or acquired without authorization.”⁶

⁴ *Id.*

⁵ *Id.*

⁶ *Id.*

32. Defendant's investigation was inconclusive whether or not the accessed data has been or will be misused by the hackers.⁷ However, upon information and belief, Toyotetsu has no methods, policies, or procedures in place that would afford its employees and customers (like Plaintiff and Class Members) any mechanism or opportunity to report misuse of the data back to Toyotetsu, and the investigation commissioned by Toyotetsu did not survey Toyotetsu's clients whose data was breached for evidence of misuse.

33. The attacker accessed, and likely acquired, files on the server containing PII, including names, addresses, and Social Security numbers.

34. On or around November 24, 2021, Defendant disclosed the Data Breach to the Maine Attorney General's Office.⁸

35. Toyotetsu first notified its impacted employees and consumers of the incident on or around November 24, 2021, sending written notifications to individuals whose personal information was compromised in the Data Breach.

36. Plaintiff's and Class Members' PII was accessed and stolen in the Data Breach.

37. Plaintiff further believes his PII, and that of Class Members, was subsequently sold on the dark web following the Data Breach, as that is the *modus operandi* of cybercriminals that commit cyber-attacks of this type

38. To prevent and detect cyber-attacks, Defendant could and should have implemented, as recommended by the United States Government, the following measures:

- Implement an awareness and training program. Because end users are targets, employees and individuals should be aware of the threat of ransomware and how it is delivered.
- Enable strong spam filters to prevent phishing emails from reaching the end users and

⁷ *Id.*

⁸ *Id.*

authenticate inbound email using technologies like Sender Policy Framework (SPF), Domain Message Authentication Reporting and Conformance (DMARC), and DomainKeys Identified Mail (DKIM) to prevent email spoofing.

- Scan all incoming and outgoing emails to detect threats and filter executable files from reaching end users.
- Configure firewalls to block access to known malicious IP addresses.
- Patch operating systems, software, and firmware on devices. Consider using a centralized patch management system.
- Set anti-virus and anti-malware programs to conduct regular scans automatically.
- Manage the use of privileged accounts based on the principle of least privilege: no users should be assigned administrative access unless absolutely needed; and those with a need for administrator accounts should only use them when necessary.
- Configure access controls—including file, directory, and network share permissions—with least privilege in mind. If a user only needs to read specific files, the user should not have write access to those files, directories, or shares.
- Disable macro scripts from office files transmitted via email. Consider using Office Viewer software to open Microsoft Office files transmitted via email instead of full office suite applications.
- Implement Software Restriction Policies (SRP) or other controls to prevent programs from executing from common ransomware locations, such as temporary folders supporting popular Internet browsers or compression/decompression programs, including the AppData/LocalAppData folder.
- Consider disabling Remote Desktop protocol (RDP) if it is not being used.
- Use application whitelisting, which only allows systems to execute programs known and permitted by security policy.
- Execute operating system environments or specific programs in a virtualized environment.
- Categorize data based on organizational value and implement physical and logical separation of networks and data for different organizational units.

39. To prevent and detect cyber-attacks, Defendant could and should have implemented, as recommended by the United States Cybersecurity & Infrastructure Security Agency, the following measures:

- **Update and patch your computer.** Ensure your applications and operating systems (OSs) have been updated with the latest patches. Vulnerable applications and OSs are the target of most ransomware attacks....
- **Use caution with links and when entering website addresses.** Be careful when clicking directly on links in emails, even if the sender appears to be someone you know. Attempt to independently verify website addresses (e.g., contact your organization's helpdesk, search the internet for the sender organization's website or the topic mentioned in the email). Pay attention to the website addresses you click on, as well as those you enter yourself. Malicious website addresses often appear almost identical to legitimate sites, often using a slight variation in spelling or a different domain (e.g., .com instead of .net)....
- **Open email attachments with caution.** Be wary of opening email attachments, even from senders you think you know, particularly when attachments are compressed files or ZIP files.
- **Keep your personal information safe.** Check a website's security to ensure the information you submit is encrypted before you provide it....
- **Verify email senders.** If you are unsure whether or not an email is legitimate, try to verify the email's legitimacy by contacting the sender directly. Do not click on any links in the email. If possible, use a previous (legitimate) email to ensure the contact information you have for the sender is authentic before you contact them.
- **Inform yourself.** Keep yourself informed about recent cybersecurity threats and up to date on ransomware techniques. You can find information about known phishing attacks on the Anti-Phishing Working Group website. You may also want to sign up for CISA product notifications, which will alert you when a new Alert, Analysis Report, Bulletin, Current Activity, or Tip has been published.
- **Use and maintain preventative software programs.** Install antivirus software, firewalls, and email filters—and keep them updated—to reduce malicious network traffic....⁹

40. To prevent and detect cyber-attacks attacks, Defendant could and should have implemented, as recommended by the Microsoft Threat Protection Intelligence Team, the following measures:

Secure internet-facing assets

- Apply latest security updates

⁹ See Security Tip (ST19-001) Protecting Against Ransomware (original release date Apr. 11, 2019), available at: <https://us-cert.cisa.gov/ncas/tips/ST19-001> (last visited Nov. 11, 2021).

- Use threat and vulnerability management
- Perform regular audit; remove privileged credentials;

Thoroughly investigate and remediate alerts

- Prioritize and treat commodity malware infections as potential full compromise;

Include IT Pros in security discussions

- Ensure collaboration among [security operations], [security admins], and [information technology] admins to configure servers and other endpoints securely;

Build credential hygiene

- Use [multifactor authentication] or [network level authentication] and use strong, randomized, just-in-time local admin passwords;

Apply principle of least-privilege

- Monitor for adversarial activities
- Hunt for brute force attempts
- Monitor for cleanup of Event Logs
- Analyze logon events;

Harden infrastructure

- Use Windows Defender Firewall
- Enable tamper protection
- Enable cloud-delivered protection
- Turn on attack surface reduction rules and [Antimalware Scan Interface] for Office [Visual Basic for Applications].¹⁰

41. Given that Defendant was storing the PII of Plaintiff and Class Members, Defendant could and should have implemented all of the above measures to prevent and detect cyber-attacks.

42. The occurrence of the Data Breach indicates that Defendant failed to adequately implement one or more of the above measures to prevent ransomware attacks, resulting in the Data

¹⁰ See Human-operated ransomware attacks: A preventable disaster (Mar 5, 2020), available at: <https://www.microsoft.com/security/blog/2020/03/05/human-operated-ransomware-attacks-a-preventable-disaster/> (last visited Nov. 11, 2021).

Breach and the exposure of the PII of an undisclosed amount of current and former consumers and employees, including Plaintiff and Class Members.

Defendant Acquires, Collects, and Stores the PII of Plaintiff and Class Members

43. Defendant has historically acquired, collected, and stored the PII of Plaintiff and Class Members.

44. As part of being a customer and/or employee of Defendant, Plaintiff and Class Members, are required to give their sensitive and confidential PII to Defendant. Defendant retains and stores this information, and derives a substantial economic benefit from the PII that it collects. But for the collection of Plaintiff's and Class Members' PII, Defendant would be unable to sell or manufacture automobile parts or employ anyone for the purpose of assisting Defendant with manufacturing car components.

45. By obtaining, collecting, and storing the PII of Plaintiff and Class Members, Defendant assumed legal and equitable duties and knew or should have known that it was responsible for protecting the PII from disclosure.

46. Plaintiff and Class Members have taken reasonable steps to maintain the confidentiality of their PII and relied on Defendant to keep their PII confidential and maintained securely, to use this information for business purposes only, and to make only authorized disclosures of this information.

47. Defendant could have prevented this Data Breach by properly securing and encrypting the files and file servers containing the PII of Plaintiff and Class Members.

48. Defendant's policies on its website include promises and legal obligations to maintain and protect PII, demonstrating an understanding of the importance of securing PII.¹¹

¹¹ <https://www.tiw.co.jp/en/privacy>

49. Defendant’s negligence in safeguarding the PII of Plaintiff and Class Members is exacerbated by the repeated warnings and alerts directed to protecting and securing sensitive data.

50. Despite the prevalence of public announcements of data breach and data security compromises, Defendant failed to take appropriate steps to protect the PII of Plaintiff and Class Members from being compromised.

Defendant Knew or Should Have Known of the Risk Because the Manufacturing Sector is Particularly Susceptible to Cyber Attacks

51. Defendant knew and understood unprotected or exposed PII in the custody of manufacturing companies, such as Defendant, is valuable and highly sought after by nefarious third parties seeking to illegally monetize that PII through unauthorized access, as these companies maintain highly sensitive PII of employees and consumers, including Social Security numbers and financial information.

Value of Personally Identifiable Information

52. The Federal Trade Commission (“FTC”) defines identity theft as “a fraud committed or attempted using the identifying information of another person without authority.”¹² The FTC describes “identifying information” as “any name or number that may be used, alone or in conjunction with any other information, to identify a specific person,” including, among other things, “[n]ame, Social Security number, date of birth, official State or government issued driver’s license or identification number, alien registration number, government passport number, employer or taxpayer identification number.”¹³

53. The PII of individuals remains of high value to criminals, as evidenced by the prices the criminals will pay through the dark web. Numerous sources cite dark web pricing for stolen

¹² 17 C.F.R. § 248.201 (2013).

¹³ *Id.*

identity credentials. For example, Personal Information can be sold at a price ranging from \$40 to \$200, and bank details have a price range of \$50 to \$200.¹⁴ Experian reports that a stolen credit or debit card number can sell for \$5 to \$110 on the dark web.¹⁵ Criminals can also purchase access to entire company data breaches from \$900 to \$4,500.¹⁶

54. Social Security numbers, for example, are among the worst kind of PII to have stolen because they may be put to a variety of fraudulent uses and are difficult for an individual to change. The Social Security Administration stresses that the loss of an individual's Social Security number, as is the case here, can lead to identity theft and extensive financial fraud:

A dishonest person who has your Social Security number can use it to get other personal information about you. Identity thieves can use your number and your good credit to apply for more credit in your name. Then, they use the credit cards and don't pay the bills, it damages your credit. You may not find out that someone is using your number until you're turned down for credit, or you begin to get calls from unknown creditors demanding payment for items you never bought. Someone illegally using your Social Security number and assuming your identity can cause a lot of problems.¹⁷

55. What is more, it is no easy task to change or cancel a stolen Social Security number. An individual cannot obtain a new Social Security number without significant paperwork and evidence of actual misuse. In other words, preventive action to defend against the possibility of misuse of a Social Security number is not permitted; an individual must show evidence of actual, ongoing fraud activity to obtain a new number.

¹⁴ *Your personal data is for sale on the dark web. Here's how much it costs*, Digital Trends, Oct. 16, 2019, available at: <https://www.digitaltrends.com/computing/personal-data-sold-on-the-dark-web-how-much-it-costs/> (last visited Jan. 19, 2022).

¹⁵ *Here's How Much Your Personal Information Is Selling for on the Dark Web*, Experian, Dec. 6, 2017, available at: <https://www.experian.com/blogs/ask-experian/heres-how-much-your-personal-information-is-selling-for-on-the-dark-web/> (last visited Jan 19, 2022).

¹⁶ *In the Dark*, VPNOverview, 2019, available at: <https://vpnoverview.com/privacy/anonymous-browsing/in-the-dark/> (last visited Jan. 19, 2022).

¹⁷ Social Security Administration, *Identity Theft and Your Social Security Number*, available at: <https://www.ssa.gov/pubs/EN-05-10064.pdf> (last visited Jan. 19, 2022).

56. Even then, a new Social Security number may not be effective. According to Julie Ferguson of the Identity Theft Resource Center, “[t]he credit bureaus and banks are able to link the new number very quickly to the old number, so all of that old bad information is quickly inherited into the new Social Security number.”¹⁸

57. Based on the foregoing, the information compromised in the Data Breach is significantly more valuable than the loss of, for example, credit card information in a retailer data breach because, there, victims can cancel or close credit and debit card accounts. The information compromised in this Data Breach is impossible to “close” and difficult, if not impossible, to change—one’s Social Security number.

58. This data demands a much higher price on the black market. Martin Walter, senior director at cybersecurity firm RedSeal, explained, “Compared to credit card information, personally identifiable information and Social Security numbers are worth more than 10x on the black market.”¹⁹

59. Among other forms of fraud, identity thieves may use Social Security numbers to obtain driver’s licenses, government benefits, medical services, and housing or even give false information to police.

60. The fraudulent activity resulting from the Data Breach may not come to light for years.

61. There may be a time lag between when harm occurs versus when it is discovered, and also between when PII is stolen and when it is used. According to the U.S. Government

¹⁸ Bryan Naylor, *Victims of Social Security Number Theft Find It’s Hard to Bounce Back*, NPR (Feb. 9, 2015), available at: <http://www.npr.org/2015/02/09/384875839/data-stolen-by-anthem-s-hackers-has-millionsworrying-about-identity-theft> (last visited Jan. 19, 2022).

¹⁹ Time Greene, *Anthem Hack: Personal Data Stolen Sells for 10x Price of Stolen Credit Card Numbers*, IT World, (Feb. 6, 2015), available at: <https://www.networkworld.com/article/2880366/anthem-hack-personal-data-stolen-sells-for-10x-price-of-stolen-credit-card-numbers.html> (last visited Nov. 11, 2021).

Accountability Office (“GAO”), which conducted a study regarding data breaches:

[L]aw enforcement officials told us that in some cases, stolen data may be held for up to a year or more before being used to commit identity theft. Further, once stolen data have been sold or posted on the Web, fraudulent use of that information may continue for years. As a result, studies that attempt to measure the harm resulting from data breaches cannot necessarily rule out all future harm.²⁰

62. At all relevant times, Defendant knew, or reasonably should have known, of the importance of safeguarding the PII of Plaintiff and Class Members, including Social Security numbers, and of the foreseeable consequences that would occur if Defendant’s data security system and network was breached, including, specifically, the significant costs that would be imposed on Plaintiff and Class Members as a result of a breach.

63. Plaintiff and Class Members now face years of constant surveillance of their financial and personal records, monitoring, and loss of rights. The Class is incurring and will continue to incur such damages in addition to any fraudulent use of their PII.

64. Defendant was, or should have been, fully aware of the unique type and the significant volume of data on Defendant’s server(s), amounting to potentially thousands of individuals’ detailed PII, and, thus, the significant number of individuals who would be harmed by the exposure of the unencrypted data.

65. In the breach notification letter, Defendant made an offer of twelve (12) months of credit and identity monitoring services. This is wholly inadequate to compensate Plaintiff and Class Members as it fails to provide for the fact that victims of data breaches and other unauthorized disclosures commonly face multiple years of ongoing identity theft and financial fraud, and it entirely fails to provide sufficient compensation for the unauthorized release and

²⁰ *Report to Congressional Requesters*, GAO, at 29 (June 2007), available at: <https://www.gao.gov/assets/gao-07-737.pdf> (last visited Jan. 19, 2022).

disclosure of Plaintiff's and Class Members' PII.

66. The injuries to Plaintiff and Class Members were directly and proximately caused by Defendant's failure to implement or maintain adequate data security measures for the PII of Plaintiff and Class Members.

67. The ramifications of Defendant's failure to keep secure the PII of Plaintiff and Class Members are long lasting and severe. Once PII is stolen, particularly Social Security numbers, fraudulent use of that information and damage to victims may continue for years.

Defendant Violated the FTC Act

68. Section 5 of the FTC Act, 15 U.S.C. § 45, prohibits "unfair . . . practices in or affecting commerce," including, as interpreted and enforced by the FTC, the unfair act or practice by businesses, such as Defendant, of failing to use reasonable measures to protect PII. The FTC publications and orders described above also form part of the basis of Defendant's duty in this regard.

69. Defendant violated Section 5 of the FTC Act by failing to use reasonable measures to protect PII and not complying with applicable industry standards, as described in detail herein. Defendant's conduct was particularly unreasonable given the nature and amount of PII it obtained and stored and the foreseeable consequences of the immense damages that would result to Plaintiff and the Nationwide Class.

Plaintiff Jonathan Phelps's Experience

70. Plaintiff was required to provide and did provide his PII to Defendant during the course of his employment with Defendant. The PII included his name, address, date of birth, Social Security Numbers, driver's license number, telephone number, and other financial and tax information.

71. To date, Toyotetsu has done next to nothing to adequately protect Plaintiff and Class Members, or to compensate them for their injuries sustained in this Data Breach.

72. Defendant's data breach notice letter downplays the theft of Plaintiff's and Class Members PII, when the facts demonstrate that the PII was targeted, accessed, and exfiltrated in a criminal cyberattack. The fraud and identity monitoring services offered by Defendant are only for one year, and it places the burden squarely on Plaintiff and Class Members by requiring them to expend time signing up for the service and addressing timely issues.

73. Plaintiff and Class Members have been further damaged by the compromise of their PII.

74. Plaintiff Phelps's PII was compromised in the Data Breach, and was likely stolen and in the hands of cybercriminals who illegally accessed Toyotetsu's network for the specific purpose of targeting the PII.

75. Plaintiff Phelps typically takes measures to protect his PII, and is very careful about sharing his PII. Phelps has never knowingly transmitted unencrypted PII over the internet or other unsecured source.

76. Plaintiff Phelps stores any documents containing his PII in a safe and secure location, and he diligently chooses unique usernames and passwords for his online accounts.

77. As a result of the Data Breach, Plaintiff has suffered a loss of time and has spent and continues to spend a considerable amount of time on issues related to this Data Breach. He monitors accounts and credit scores and has sustained emotional distress. This is time that was lost and unproductive and took away from other activities and duties.

78. Plaintiff has recently experienced fraudulent charges on a credit card account to which he is an authorized user, totaling approximately \$300.00.

79. Plaintiff also suffered actual injury in the form of damages to and diminution in the value of his PII—a form of intangible property that he entrusted to Defendant for the purpose of obtaining employment from Defendant, which was compromised in and as a result of the Data Breach.

80. Plaintiff suffered lost time, annoyance, interference, and inconvenience as a result of the Data Breach and has anxiety and increased concerns for the loss of his privacy.

81. Plaintiff has suffered imminent and impending injury arising from the substantially increased risk of fraud, identity theft, and misuse resulting from his PII, especially his Social Security Number, being placed in the hands of criminals.

82. Defendant obtained and continues to maintain Plaintiff's PII and has a continuing legal duty and obligation to protect that PII from unauthorized access and disclosure. Defendant required the PII from Plaintiff when he began employment with Defendant. Plaintiff, however, would not have entrusted his PII to Defendant had he known that it would fail to maintain adequate data security. Plaintiff's PII was compromised and disclosed as a result of the Data Breach.

83. As a result of the Data Breach, Plaintiff anticipates spending considerable time and money on an ongoing basis to try to mitigate and address harms caused by the Data Breach. As a result of the Data Breach, Plaintiff is at a present risk and will continue to be at increased risk of identity theft and fraud for years to come.

CLASS ALLEGATIONS

84. Plaintiff brings this suit on behalf of himself and a class of similarly situated individuals under Kentucky Rule of Civil Procedure 23.01, *et seq.*, which is preliminarily defined as:

All persons Toyotetsu North America identified as being among those individuals impacted by the Data Breach, including all who were sent a notice

of the Data Breach.

85. Excluded from the Classes are the following individuals and/or entities: Defendant and Defendant's parents, subsidiaries, affiliates, officers and directors, and any entity in which Defendant has a controlling interest; all individuals who make a timely election to be excluded from this proceeding using the correct protocol for opting out; and all judges assigned to hear any aspect of this litigation, as well as their immediate family members.

86. **Numerosity.** The Class Members are so numerous that joinder of all members is impracticable. Though the exact number and identities of Class Members are unknown at this time, reports indicate that approximately 12,450 individuals had their PII compromised in this Data Breach. The identities of Class Members are ascertainable through Toyotetsu's records, Class Members' records, publication notice, self-identification, and other means.

87. **Commonality.** There are questions of law and fact common to the Class, which predominate over any questions affecting only individual Class Members. These common questions of law and fact include, without limitation:

- a. Whether Toyotetsu unlawfully used, maintained, lost, or disclosed Plaintiff's and Class Members' PII;
- b. Whether Toyotetsu failed to implement and maintain reasonable security procedures and practices appropriate to the nature and scope of the information compromised in the Data Breach;
- c. Whether Toyotetsu data security systems prior to and during the Data Breach complied with applicable data security laws and regulations;
- d. Whether Toyotetsu data security systems prior to and during the Data Breach were consistent with industry standards;

- e. Whether Toyotetsu owed a duty to Class Members to safeguard their PII;
- f. Whether Toyotetsu breached its duty to Class Members to safeguard their PII;
- g. Whether computer hackers obtained Class Members' PII in the Data Breach;
- h. Whether Toyotetsu knew or should have known that its data security systems and monitoring processes were deficient;
- i. Whether Plaintiff and Class Members suffered legally cognizable damages as a result of Toyotetsu's misconduct;
- j. Whether Toyotetsu's conduct was negligent;
- k. Whether Toyotetsu's conduct was *per se* negligent, and;
- l. Whether Plaintiff and Class Members are entitled to damages, civil penalties, punitive damages, and/or injunctive relief.

88. **Typicality.** Plaintiff's claims are typical of those of other Class Members because Plaintiff's PII, like that of every other Class member, was compromised in the Data Breach.

89. **Adequacy of Representation.** Plaintiff will fairly and adequately represent and protect the interests of the Members of the Class. Plaintiff's Counsel is competent and experienced in litigating Class actions, including data privacy litigation of this kind.

90. **Predominance.** Toyotetsu has engaged in a common course of conduct toward Plaintiff and Class Members, in that all the Plaintiff's and Class Members' data was stored on the same computer systems and unlawfully accessed in the same way. The common issues arising from Defendant's conduct affecting Class Members set out above predominate over any individualized issues. Adjudication of these common issues in a single action has important and desirable advantages of judicial economy.

91. **Superiority.** A Class action is superior to other available methods for the fair and

efficient adjudication of the controversy. Class treatment of common questions of law and fact is superior to multiple individual actions or piecemeal litigation. Absent a Class action, most Class Members would likely find that the cost of litigating their individual claims is prohibitively high and would therefore have no effective remedy. The prosecution of separate actions by individual Class Members would create a risk of inconsistent or varying adjudications with respect to individual Class Members, which would establish incompatible standards of conduct for Toyotetsu. In contrast, the conduct of this action as a Class action presents far fewer management difficulties, conserves judicial resources and the parties' resources, and protects the rights of each Class member.

92. Toyotetsu has acted on grounds that apply generally to the Class as a whole, so that Class certification, injunctive relief, and corresponding declaratory relief are appropriate on a Class-wide basis.

93. Likewise, particular issues are appropriate for certification because such claims present only particular, common issues, the resolution of which would advance the disposition of this matter and the parties' interests therein. Such particular issues include, but are not limited to:

- m. Whether Toyotetsu owed a legal duty to Plaintiff and the Class to exercise due care in collecting, storing, and safeguarding their PII;
- n. Whether Toyotetsu's security measures to protect its data systems were reasonable in light of best practices recommended by data security experts;
- o. Whether Toyotetsu's failure to institute adequate protective security measures amounted to negligence;
- p. Whether Toyotetsu failed to take commercially reasonable steps to safeguard employee and consumer PII; and

q. Whether adherence to FTC data security recommendations, and measures recommended by data security experts would have reasonably prevented the data breach.

94. Finally, all members of the proposed Class are readily ascertainable. Toyotetsu has access to Class Members' names and addresses affected by the Data Breach. Class Members have already been preliminarily identified and sent notice of the Data Breach by Toyotetsu.

FIRST CAUSE OF ACTION
NEGLIGENCE
(On Behalf of Plaintiff and the Class)

95. Plaintiff incorporates by reference all other allegations in the Complaint as if fully set forth herein.

96. Toyotetsu knowingly collected, came into possession of, and maintained Plaintiff's and Class Members' PII, and had a duty to exercise reasonable care in safeguarding, securing, and protecting such information from being compromised, lost, stolen, misused, and/or disclosed to unauthorized parties.

97. Toyotetsu had a duty under common law to have procedures in place to detect and prevent the loss or unauthorized dissemination of Plaintiff's and Class Members' PII.

98. Defendant had full knowledge of the sensitivity of the PII and the types of harm that Plaintiff and Class Members could and would suffer if the PII were wrongfully disclosed.

99. By assuming the responsibility to collect and store this data, and in fact doing so, and sharing it and using it for commercial gain, Defendant had a duty of care to use reasonable means to secure and safeguard its computer property—and Class Members' PII held within it—to prevent disclosure of the information, and to safeguard the information from theft. Defendant's duty included a responsibility to implement processes by which they could detect a breach of its

security systems in a reasonably expeditious period of time and to give prompt notice to those affected in the case of a data breach.

100. Toyotetsu had a duty to employ reasonable security measures under Section 5 of the Federal Trade Commission Act, 15 U.S.C. § 45, which prohibits “unfair. . . practices in or affecting commerce,” including, as interpreted and enforced by the FTC, the unfair practice of failing to use reasonable measures to protect confidential data.

101. Toyotetsu had a duty to employ reasonable security measures and otherwise protect the PII of Plaintiff and Class Members pursuant to in K.R.S. § 365.720 - § 365.732.

102. Toyotetsu, through its actions and/or omissions, unlawfully breached its duty to Plaintiff and Class members by failing to exercise reasonable care in protecting and safeguarding Plaintiff’s and Class Members’ PII within Toyotetsu’s possession.

103. Toyotetsu, through its actions and/or omissions, unlawfully breached its duty to Plaintiff and Class members by failing to have appropriate procedures in place to detect and prevent dissemination of Plaintiff’s and Class Members’ PII.

104. Toyotetsu, through its actions and/or omissions, unlawfully breached its duty to timely disclose to Plaintiff and Class Members that the PII within Toyotetsu s’ possession might have been compromised and precisely the type of information compromised.

105. Toyotetsu’s breach of duties owed to Plaintiff and Class Members caused Plaintiff’s and Class Members’ PII to be compromised.

106. As a result of Toyotetsu’s ongoing failure to notify Plaintiff and Class Members regarding the type of PII has been compromised, Plaintiff and Class Members are unable to take the necessary precautions to mitigate damages by preventing future fraud.

107. Toyotetsu's breaches of duty caused Plaintiff and Class Members to suffer from identity theft, loss of time and money to monitor their finances for fraud, and loss of control over their PII.

108. As a result of Toyotetsu's negligence and breach of duties, Plaintiff and Class Members are in danger of imminent harm in that their PII, which is still in the possession of third parties, will be used for fraudulent purposes.

109. Plaintiff seeks the award of actual damages on behalf of himself and the Class.

110. In failing to secure Plaintiff's and Class Members' PII and promptly notifying them of the Data Breach, Toyotetsu is guilty of oppression, fraud, or malice, in that Toyotetsu acted or failed to act with a willful and conscious disregard of Plaintiff's and Class Members' rights. Plaintiff, therefore, in addition to seeking actual damages, seeks punitive damages on behalf of himself and the Class.

111. Plaintiff seeks injunctive relief on behalf of the Class in the form of an order compelling Toyotetsu to institute appropriate data collection and safeguarding methods and policies with regard to patient information.

SECOND CAUSE OF ACTION
BREACH OF IMPLIED CONTRACT
(On Behalf of Plaintiff and the Class)

112. Plaintiff incorporates by reference all other allegations in the Complaint as if fully set forth herein.

113. Plaintiff and Class Members were required to provide their PII to Defendant as a condition of employment or use of Defendant's services.

114. Plaintiff and Class Members disclosed their PII in exchange for employment, along with Defendant's promise to protect their PII from unauthorized disclosure.

115. In its written privacy policies, Defendant Toyotetsu expressly promised Plaintiff and Class Members that it would only disclose PII under certain circumstances, none of which relate to the Data Breach.

116. Defendant further promised to comply with industry standards and to make sure that Plaintiff's and Class Members' PII would remain protected.

117. There was a meeting of the minds and an implied contractual agreement between Plaintiff and Class Members and the Defendant, under which Plaintiff and Class Members would provide their PII in exchange for Defendant's obligations to: (a) use such PII for business purposes only, (b) take reasonable steps to safeguard that PII, (c) prevent unauthorized disclosures of the PII, (d) provide Plaintiff and Class Members with prompt and sufficient notice of any and all unauthorized access and/or theft of their PII, (e) reasonably safeguard and protect the PII of Plaintiff and Class Members from unauthorized disclosure or uses, (f) retain the PII only under conditions that kept such information secure and confidential.

118. When Plaintiff and Class Members provided their PII to Defendant Toyotetsu as a condition of obtaining Toyotetsu employment, or as a condition precedent to receiving Toyotetsu services, they entered into implied contracts with Defendant pursuant to which Defendant agreed to reasonably protect such information.

119. Defendant solicited, invited, and then required Class Members to provide their PII as part of Defendant's regular business practices. Plaintiff and Class Members accepted Defendant's offers and provided their PII to Defendant.

120. In entering into such implied contracts, Plaintiff and Class Members reasonably believed and expected that Defendant's data security practices complied with relevant laws and regulations and were consistent with industry standards.

121. Plaintiff and Class Members would not have entrusted their PII to Defendant in the absence of the implied contract between them and Defendant to keep their information reasonably secure. Plaintiff and Class Members would not have entrusted their PII to Defendant in the absence of its implied promise to monitor its computer systems and networks to ensure that it adopted reasonable data security measures.

122. Plaintiff and Class Members fully and adequately performed their obligations under the implied contracts with Defendant.

123. Defendant breached its implied contracts with Class Members by failing to safeguard and protect their PII.

124. As a direct and proximate result of Defendant breaches of the implied contracts, Class Members sustained damages as alleged herein.

125. Plaintiff and Class Members are entitled to compensatory and consequential damages suffered as a result of the Data Breach.

126. Plaintiff and Class Members are also entitled to injunctive relief requiring Defendant to, e.g., (i) strengthen its data security systems and monitoring procedures; (ii) submit to future annual audits of those systems and monitoring procedures; and (iii) immediately provide adequate credit monitoring to all Class Members.

THIRD CAUSE OF ACTION
UNJUST ENRICHMENT
(On Behalf of Plaintiff and the Class)

127. Plaintiff incorporates by reference all other allegations in the Complaint as if fully set forth herein.

128. This claim is plead in the alternative to the Second Cause of Action for breach of implied contract.

129. Defendant benefited from receiving Plaintiff's and Class Members' PII by its ability to retain and use that information for its own benefit. Defendant understood this benefit.

130. Defendant also understood and appreciated that Plaintiff's and Class Members' PII was private and confidential, and its value depended upon Defendant maintaining the privacy and confidentiality of that information.

131. Plaintiff and Class Members conferred a monetary benefit upon Defendant in the form of purchasing services from Defendant, and in connection thereto, by providing their PII to Defendant with the understanding that Defendant would pay for the administrative costs of reasonable data privacy and security practices and procedures. Specifically, they were required to provide Defendant with their PII. In exchange, Plaintiff and Class members should have received adequate protection and data security for such PII held by Defendant.

132. Defendant knew Plaintiff and Class members conferred a benefit which Defendant accepted. Defendant profited from these transactions and used the PII of Plaintiff and Class Members for business purposes.

133. Defendant failed to provide reasonable security, safeguards, and protections to the PII of Plaintiff and Class Members.

134. Under the principles of equity and good conscience, Defendant should not be permitted to retain money belonging to Plaintiff and Class Members, because Defendant failed to implement appropriate data management and security measures mandated by industry standards.

135. Defendant wrongfully accepted and retained these benefits to the detriment of Plaintiff and Class Members.

136. Defendant's enrichment at the expense of Plaintiff and Class Members is and was unjust.

137. As a result of Defendant’s wrongful conduct, as alleged above, Plaintiff and the Class Members are entitled to restitution and disgorgement of all profits, benefits, and other compensation obtained by Defendant, plus attorneys’ fees, costs, and interest thereon.

FOURTH CAUSE OF ACTION
NEGLIGENCE *PER SE*
(On Behalf of Plaintiff and the Class)

138. Plaintiff incorporates by reference all other allegations in the Complaint as if fully set forth herein.

139. Section 5 of the FTC Act, 15 U.S.C. § 45, prohibits “unfair . . . practices in or affecting commerce” including, as interpreted and enforced by the FTC, the unfair act or practice by Defendant of failing to use reasonable measures to protect PII. Various FTC publications and orders also form the basis of Defendant’s duty.

140. Defendant violated Section 5 of the FTC Act (and similar state statutes) by failing to use reasonable measures to protect PII and not complying with industry standards. Defendant’s conduct was particularly unreasonable given the nature and amount of PII obtained and stored and the foreseeable consequences of a data breach on Defendant’s systems.

141. Defendant’s violation of Section 5 of the FTC Act (and similar state statutes) constitutes negligence per se.

142. The harm that has occurred is the type of harm the FTC Act (and similar state statutes) was intended to guard against. Indeed, the FTC has pursued over fifty enforcement actions against businesses which, as a result of their failure to employ reasonable data security measures and avoid unfair and deceptive practices, caused the same harm suffered by Plaintiff and Class Members.

143. As a direct and proximate result of Defendant Toyotetsu’s negligence, Plaintiff and Class Members have been injured and are 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 their 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 their bargains and overcharges for services; and other economic and non-economic harm.

PRAYER FOR RELIEF

WHEREFORE, Plaintiff, on behalf of himself and Class Members, request judgment against Defendant and that the Court grant the following:

- A. For an order certifying the Class, as defined herein, and appointing Plaintiff and his Counsel to represent each such Class;
- B. For equitable relief enjoining Defendant from engaging in the wrongful conduct complained of herein pertaining to the misuse and/or disclosure of the PII of Plaintiff and Class Members, and from refusing to issue prompt, complete, any accurate disclosures to Plaintiff and Class Members;
- C. For injunctive relief requested by Plaintiff, including but not limited to, injunctive and other equitable relief as is necessary to protect the interests of Plaintiff and Class Members, including but not limited to an order:
 - i. prohibiting Defendant from engaging in the wrongful and unlawful acts

- described herein;
- ii. requiring Defendant to protect, including through encryption, all data collected through the course of its business in accordance with all applicable regulations, industry standards, and federal, state, or local laws;
 - iii. requiring Defendant to delete, destroy, and purge the personal identifying information of Plaintiff and Class Members unless Defendant can provide to the Court reasonable justification for the retention and use of such information when weighed against the privacy interests of Plaintiff and Class Members;
 - iv. requiring Defendant to implement and maintain a comprehensive Information Security Program designed to protect the confidentiality and integrity of the PII of Plaintiff and Class Members;
 - v. prohibiting Defendant from maintaining the PII of Plaintiff and Class Members on a cloud-based database;
 - vi. requiring Defendant to engage independent third-party security auditors/penetration testers as well as internal security personnel to conduct testing, including simulated attacks, penetration tests, and audits on Defendant's systems on a periodic basis, and ordering Defendant to promptly correct any problems or issues detected by such third-party security auditors;
 - vii. requiring Defendant to engage independent third-party security auditors and internal personnel to run automated security monitoring;
 - viii. requiring Defendant to audit, test, and train its security personnel regarding any new or modified procedures;
 - ix. requiring Defendant to segment data by, among other things, creating firewalls

and access controls so that if one area of Defendant's network is compromised, hackers cannot gain access to other portions of Defendant's systems;

- x. requiring Defendant to conduct regular database scanning and securing checks;
- xi. requiring Defendant to establish an information security training program that includes at least annual information security training for all employees, with additional training to be provided as appropriate based upon the employees' respective responsibilities with handling personal identifying information, as well as protecting the personal identifying information of Plaintiff and Class Members;
- xii. requiring Defendant to conduct internal training and education routinely and continually, and on an annual basis to inform internal security personnel how to identify and contain a breach when it occurs and what to do in response to a breach;
- xiii. requiring Defendant to implement a system of tests to assess its employees' knowledge of the education programs discussed in the preceding subparagraphs, as well as randomly and periodically testing employees' compliance with Defendant's policies, programs, and systems for protecting personal identifying information;
- xiv. requiring Defendant to implement, maintain, regularly review, and revise as necessary a threat management program designed to appropriately monitor Defendant's information networks for threats, both internal and external, and assess whether monitoring tools are appropriately configured, tested, and updated;

- xv. requiring Defendant to meaningfully educate all Class Members about the threats that they face as a result of the loss of their confidential PII to third parties, as well as the steps affected individuals must take to protect themselves;
 - xvi. requiring Defendant to implement logging and monitoring programs sufficient to track traffic to and from Defendant's servers; and for a period of 10 years, appointing a qualified and independent third-party assessor to conduct a SOC 2 Type 2 attestation on an annual basis to evaluate Defendant's compliance with the terms of the Court's final judgment, to provide such report to the Court and to counsel for the class, and to report any deficiencies with compliance of the Court's final judgment;
- D. For an award of damages, including actual, statutory, nominal, and consequential damages, as allowed by law in an amount to be determined;
 - E. For an award of attorneys' fees, costs, and litigation expenses, as allowed by law;
 - F. For prejudgment interest on all amounts awarded; and
 - G. Such other and further relief as this Court may deem just and proper.

DEMAND FOR JURY TRIAL

Plaintiff hereby demands that this matter be tried before a jury.

Respectfully submitted,

Terence R. Coates (*pro hac vice* forthcoming)
MARKOVITS, STOCK & DEMARCO, LLC
3825 Edwards Road, Suite 650
Cincinnati, OH 45209
Phone: (513) 651-3700
Fax: (513) 665-0219
tcoates@msdlegal.com
Counsel for Plaintiff and the Class

and

Joseph B. Venters
VENTERS LAW OFFICE
P.O. Box 1749
Somerset, KY 42502
Phone: (606) 451-0332
Fax: (606) 451-0335
joey@venterslaw.com
Co-Counsel for Plaintiff and the Class

AOC-E-105 Sum Code: CI
Rev. 9-14

Commonwealth of Kentucky
Court of Justice Courts.ky.gov

CR 4.02; Cr Official Form 1



Case #: 22-CI-00328

Court: CIRCUIT

County: PULASKI

CIVIL SUMMONS

Plaintiff, **PHELPS, JONATHAN VS. TOYOTETSU NORTH AMERICA**, Defendant

TO: **GREGORY A. COWAN**
100 PIN OAK DRIVE
SOMERSET, KY 42503

Memo: Related party is TOYOTETSU NORTH AMERICA

The Commonwealth of Kentucky to Defendant:
TOYOTETSU NORTH AMERICA

You are hereby notified that a **legal action has been filed against you** in this Court demanding relief as shown on the document delivered to you with this Summons. **Unless a written defense is made by you or by an attorney on your behalf within twenty (20) days** following the day this paper is delivered to you, judgment by default may be taken against you for the relief demanded in the attached complaint.

The name(s) and address(es) of the party or parties demanding relief against you or his/her (their) attorney(s) are shown on the document delivered to you with this Summons.

/s/ Eliza York-Hansel,
Pulaski Circuit Special Clerk
Date: 4/14/2022

Proof of Service

This Summons was:

Served by delivering a true copy and the Complaint (or other initiating document)

To: Gregory Cowan

Not Served because: _____

Date: 4-15, 2022

D. Weddle
Served By

Constable
Title

Summons ID: @00000188433
CIRCUIT: 22-CI-00328 Return to Filer for Service
PHELPS, JONATHAN VS. TOYOTETSU NORTH AMERICA



COMMONWEALTH OF KENTUCKY
28TH JUDICIAL CIRCUIT
PULASKI CIRCUIT COURT
CIVIL ACTION NO. 22-CI-_____

JONATHAN PHELPS, individually and
on behalf of all others similarly situated

PLAINTIFF

vs.

TOYOTETSU NORTH AMERICA
Serve By: Constable
Registered Agent: Gregroy A. Cowan
100 Pin Oak Drive
Somerset, Kentucky 42503

DEFENDANT

CLASS ACTION CIVIL COMPLAINT

Plaintiff JONATHAN PHELPS (“Plaintiff”) brings this Class Action Complaint against TOYOTETSU NORTH AMERICA (“Defendant” or “Toyotetsu”), in his individual capacity and on behalf of all others similarly situated, and alleges, upon personal knowledge as to his own actions and his counsels’ investigations, and upon information and belief as to all other matters, as follows:

I. INTRODUCTION

1. This class action arises out of the recent data breach (“Data Breach”) involving Defendant Toyotetsu, a for-profit manufacturer of car components located in Somerset, Kentucky
2. Toyotetsu failed to reasonably secure, monitor, and maintain Personally Identifiable Information (“PII”) provided by employees and consumers, including, without limitation, full names, addresses, and Social Security numbers of individuals stored on its private network. As a result, Plaintiff and other impacted individuals suffered present injury and damages in the form of identity theft, loss of value of their PII, out-of-pocket expenses and the value of their time reasonably incurred to remedy or mitigate the effects of the unauthorized access, exfiltration, and

subsequent criminal misuse of their sensitive and highly personal information.

3. Moreover, after learning of the Data Breach, Defendant waited nearly two months to notify Plaintiff and Class Members of the Data Breach and/or inform them that their PII was compromised. During this time, Plaintiff and Class Members were unaware that their sensitive PII had been compromised, and that they were, and continue to be, at significant risk of identity theft and various other forms of personal, social, and financial harm.

4. By obtaining, collecting, using, and deriving a benefit from the PII of Plaintiff and Class Members, Defendant assumed legal and equitable duties to those individuals to protect and safeguard that information from unauthorized access and intrusion. Defendant's conduct in breaching these duties amounts to negligence and/or recklessness and violates federal and state statutes.

5. Plaintiff brings this action on behalf of all persons whose PII was compromised as a result of Defendant's failure to take reasonable steps to protect the PII of Plaintiff and Class Members and warn Plaintiff and Class Members of Defendant's inadequate information security practices. Defendant disregarded the rights of Plaintiff and Class Members by knowingly failing to implement and maintain adequate and reasonable measures to ensure that the PII of Plaintiff and Class Members was safeguarded, failing to take available steps to prevent an unauthorized disclosure of data, and failing to follow applicable, required, and appropriate protocols, policies, and procedures regarding the encryption of data, even for internal use.

6. As a direct and proximate result of Defendant's data security failures and the Data Breach, the PII of Plaintiff and Class Members was compromised through disclosure to an unknown and unauthorized third party, and Plaintiff and Class Members have suffered actual, present, concrete injuries. These injuries include: (i) the current and imminent risk of fraud and

identity theft (ii) lost or diminished value of PII ; (iii) out-of-pocket expenses associated with the prevention, detection, and recovery from identity theft, tax fraud, and/or unauthorized use of their PII; (iv) lost opportunity costs associated with attempting to mitigate the actual consequences of the Data Breach, including but not limited to lost time; and (v) the continued and certainly increased risk to their PII, which: (a) remains unencrypted and available for unauthorized third parties to access and abuse; and (b) may remain backed up in Defendant’s possession and is subject to further unauthorized disclosures so long as Defendant fails to undertake appropriate and adequate measures to protect the PII; (vi) the invasion of privacy; (vii) the compromise, disclosure, theft, and unauthorized use of Plaintiff’s and the Class Members’ PII; and (viii) emotional distress, fear, anxiety, nuisance and annoyance related to the theft and compromise of their PII.

7. Plaintiff and Class Members seek to remedy these harms and prevent any future data compromise on behalf of themselves and all similarly situated persons whose personal data was compromised and stolen as a result of the Data Breach and remains at risk due to inadequate data security.

8. Plaintiff and Class Members have a continuing interest in ensuring that their information is and remains safe, and they should be entitled to injunctive and other equitable relief.

II. PARTIES

Plaintiff Jonathan Phelps

9. Plaintiff Jonathan Phelps is, and at all times relevant has been, a resident and citizen of Kentucky, where he intends to remain. Plaintiff received a “Notice of Security” letter, dated November 24, 2021, on or about that date. The letter notified Plaintiff that on October 7, 2021, Toyotetsu identified unusual activity on its network and that “certain files containing personal

information may have been accessed or acquired without authorization.”¹ The type of data at issue included full names, addresses, and Social Security numbers.² The letter further advised that Plaintiff that he could participate in credit monitoring services detecting suspicious activity.

10. Defendant obtained and continues to maintain Plaintiff’s and Class Members’ PII and has a continuing legal duty and obligation to protect that sensitive information from unauthorized access and disclosure. Defendant required the PII from Plaintiff. Plaintiff, however, would not have entrusted his PII to Defendant had he known that it would fail to maintain adequate data security. Plaintiff’s PII was compromised and disclosed as a result of the Data Breach.

Defendant Toyotetsu North America

11. Defendant Toyotetsu is Kentucky corporation headquartered in and with a principal office location of 100 Pin Oak Drive, Somerset, Kentucky 42503. Toyotetsu is a manufacturer of car components that was established in Somerset, KY in 1995, and began production in 1997. Toyotetsu’s customers include Toyota Motor Manufacturing Kentucky, Nissan, and Subaru.

12. All of Plaintiff’s claims stated herein are asserted against Defendant and any of its owners, predecessors, successors, subsidiaries, agents and/or assigns.

III. JURISDICTION AND VENUE

13. This Court has subject matter jurisdiction pursuant to the Class Action Fairness Act of 2005 (“CAFA”), 28 U.S.C. § 1332(d). The amount in controversy exceeds the sum of \$5,000,000 exclusive of interest and costs, there are more than 100 putative class members, and minimal diversity exists because many putative class members are citizens of a different state than

¹ <https://apps.web.maine.gov/online/aeviewer/ME/40/275fde84-6559-4ed0-9ba4-a7a4a3d75dee.shtml>

² *Id.*

Defendant. This Court also has supplemental jurisdiction pursuant to 28 U.S.C. § 1367(a) because all claims alleged herein form part of the same case or controversy.

14. This Court has personal jurisdiction over Toyotetsu because it is headquartered in and maintains its principal place of business in this county. Toyotetsu is authorized to and regularly conducts business in Kentucky.

15. This Court has jurisdiction over the parties and over the subject matter by virtue of KRS Chapter 338; KRS 446.070; KRS 411.184(2); and because the amount in dispute exceeds the minimum dollar amount needed to establish jurisdiction in this Court.

16. This Court is the proper place of venue pursuant to KRS Chapter 338; KRS 446.070; KRS 411.184(2); and because all the unlawful acts and/or unlawful omissions complained herein all occurred in Somerset, Kentucky.

IV. FACTUAL ALLEGATIONS

Background

17. Defendant is a manufacturer of car components that was established in Somerset, KY with customers that include Toyota Motor Manufacturing Kentucky, Nissan, and Subaru.

18. Plaintiff and Class Members were customers and/or employees of Defendant whose PII was required to be provided, and was in fact provided, to Defendant in conjunction with manufacturing of car components or during the course of their employment with Defendant. Plaintiff's and Class Members' PII were required to fill out various forms, including without limitation employment paperwork and applications, tax documents, various authorizations, other form documents associated with the manufacturing of car components, and employment documentation.

19. Plaintiff and Class Members relied on the sophistication of Defendant and its network to keep their PII confidential and securely maintained, to use this information for business and/or employment purposes only, and to make only authorized disclosures of this information. Plaintiff and Class Members demand security to safeguard their PII.

20. Defendant required the submission of and voluntarily accepted the PII as part of its business and had a duty to adopt reasonable measures to protect the PII of Plaintiff and Class Members from involuntary disclosure to third parties. Toyotetsu has a legal duty to keep employee and consumer PII safe and confidential.

21. The information held by Defendant in its computer systems and networks included the PII of Plaintiff and Class Members.

22. Defendant derived a substantial economic benefit from collecting Plaintiff's and Class Members' PII.

23. By obtaining, collecting, using, and deriving a benefit from Plaintiff's and Class Members' PII, Toyotetsu assumed legal and equitable duties and knew or should have known that it was responsible for protecting Plaintiff's and Class Members' PII from disclosure.

24. Plaintiff and the Class Members have taken reasonable steps to maintain the confidentiality of their PII.

The Data Breach

25. "On October 7, 2021, Toyotetsu detected unusual network activity impacting certain systems."³

26. According to Defendant, Toyotetsu alleges that it conducted "an investigation to determine what happened and whether any personal information was accessed or acquired without

³ <https://apps.web.maine.gov/online/aeviewer/ME/40/275fde84-6559-4ed0-9ba4-a7a4a3d75dec.shtml>

authorization as a result. Through the investigation, Toyotetsu learned that certain files containing personal information may have been accessed or acquired without authorization.”⁴

27. To date, Toyotetsu has not revealed when the unauthorized actor first gained access to a portion of Defendant’s network, nor has it revealed the mechanism by which the unauthorized actor first gained access to Defendant’s network.

28. Upon information and belief, the unauthorized actor gained access to Toyotetsu’s network well in advance of the October 7, 2021 date that the intrusion was first discovered by Toyotetsu, meaning that the unauthorized actor had unfettered and undetected access to Defendant’s networks for a considerable period of time prior to Toyotetsu becoming aware of the unauthorized access to its computer systems and network.

29. After Toyotetsu initially discovery the unauthorized access to its systems, Toyotetsu commissioned computer forensic specialists to conduct an investigation to determine the nature and scope of the event.

30. The investigation commissioned by Toyotetsu did not conclude until November 16, 2021, and notice was not sent to victims of the data breach at least a week after that.⁵ Thus, the victims of this Data Breach, including Plaintiff and Class Members, were not sent notice of this Data Breach until approximately eight weeks after Toyotetsu first knew about this Data Breach.

31. Defendant acknowledged that “certain files containing personal information may have been accessed or acquired without authorization.”⁶

⁴ *Id.*
⁵ *Id.*
⁶ *Id.*

32. Defendant's investigation was inconclusive whether or not the accessed data has been or will be misused by the hackers.⁷ However, upon information and belief, Toyotetsu has no methods, policies, or procedures in place that would afford its employees and customers (like Plaintiff and Class Members) any mechanism or opportunity to report misuse of the data back to Toyotetsu, and the investigation commissioned by Toyotetsu did not survey Toyotetsu's clients whose data was breached for evidence of misuse.

33. The attacker accessed, and likely acquired, files on the server containing PII, including names, addresses, and Social Security numbers.

34. On or around November 24, 2021, Defendant disclosed the Data Breach to the Maine Attorney General's Office.⁸

35. Toyotetsu first notified its impacted employees and consumers of the incident on or around November 24, 2021, sending written notifications to individuals whose personal information was compromised in the Data Breach.

36. Plaintiff's and Class Members' PII was accessed and stolen in the Data Breach.

37. Plaintiff further believes his PII, and that of Class Members, was subsequently sold on the dark web following the Data Breach, as that is the *modus operandi* of cybercriminals that commit cyber-attacks of this type

38. To prevent and detect cyber-attacks, Defendant could and should have implemented, as recommended by the United States Government, the following measures:

- Implement an awareness and training program. Because end users are targets, employees and individuals should be aware of the threat of ransomware and how it is delivered.
- Enable strong spam filters to prevent phishing emails from reaching the end users and

⁷ *Id.*

⁸ *Id.*

authenticate inbound email using technologies like Sender Policy Framework (SPF), Domain Message Authentication Reporting and Conformance (DMARC), and DomainKeys Identified Mail (DKIM) to prevent email spoofing.

- Scan all incoming and outgoing emails to detect threats and filter executable files from reaching end users.
- Configure firewalls to block access to known malicious IP addresses.
- Patch operating systems, software, and firmware on devices. Consider using a centralized patch management system.
- Set anti-virus and anti-malware programs to conduct regular scans automatically.
- Manage the use of privileged accounts based on the principle of least privilege: no users should be assigned administrative access unless absolutely needed; and those with a need for administrator accounts should only use them when necessary.
- Configure access controls—including file, directory, and network share permissions—with least privilege in mind. If a user only needs to read specific files, the user should not have write access to those files, directories, or shares.
- Disable macro scripts from office files transmitted via email. Consider using Office Viewer software to open Microsoft Office files transmitted via email instead of full office suite applications.
- Implement Software Restriction Policies (SRP) or other controls to prevent programs from executing from common ransomware locations, such as temporary folders supporting popular Internet browsers or compression/decompression programs, including the AppData/LocalAppData folder.
- Consider disabling Remote Desktop protocol (RDP) if it is not being used.
- Use application whitelisting, which only allows systems to execute programs known and permitted by security policy.
- Execute operating system environments or specific programs in a virtualized environment.
- Categorize data based on organizational value and implement physical and logical separation of networks and data for different organizational units.

39. To prevent and detect cyber-attacks, Defendant could and should have implemented, as recommended by the United States Cybersecurity & Infrastructure Security Agency, the following measures:

- **Update and patch your computer.** Ensure your applications and operating systems (OSs) have been updated with the latest patches. Vulnerable applications and OSs are the target of most ransomware attacks....
- **Use caution with links and when entering website addresses.** Be careful when clicking directly on links in emails, even if the sender appears to be someone you know. Attempt to independently verify website addresses (e.g., contact your organization's helpdesk, search the internet for the sender organization's website or the topic mentioned in the email). Pay attention to the website addresses you click on, as well as those you enter yourself. Malicious website addresses often appear almost identical to legitimate sites, often using a slight variation in spelling or a different domain (e.g., .com instead of .net)....
- **Open email attachments with caution.** Be wary of opening email attachments, even from senders you think you know, particularly when attachments are compressed files or ZIP files.
- **Keep your personal information safe.** Check a website's security to ensure the information you submit is encrypted before you provide it....
- **Verify email senders.** If you are unsure whether or not an email is legitimate, try to verify the email's legitimacy by contacting the sender directly. Do not click on any links in the email. If possible, use a previous (legitimate) email to ensure the contact information you have for the sender is authentic before you contact them.
- **Inform yourself.** Keep yourself informed about recent cybersecurity threats and up to date on ransomware techniques. You can find information about known phishing attacks on the Anti-Phishing Working Group website. You may also want to sign up for CISA product notifications, which will alert you when a new Alert, Analysis Report, Bulletin, Current Activity, or Tip has been published.
- **Use and maintain preventative software programs.** Install antivirus software, firewalls, and email filters—and keep them updated—to reduce malicious network traffic....⁹

40. To prevent and detect cyber-attacks attacks, Defendant could and should have implemented, as recommended by the Microsoft Threat Protection Intelligence Team, the following measures:

Secure internet-facing assets

- Apply latest security updates

⁹ See Security Tip (ST19-001) Protecting Against Ransomware (original release date Apr. 11, 2019), available at: <https://us-cert.cisa.gov/ncas/tips/ST19-001> (last visited Nov. 11, 2021).

- Use threat and vulnerability management
- Perform regular audit; remove privileged credentials;

Thoroughly investigate and remediate alerts

- Prioritize and treat commodity malware infections as potential full compromise;

Include IT Pros in security discussions

- Ensure collaboration among [security operations], [security admins], and [information technology] admins to configure servers and other endpoints securely;

Build credential hygiene

- Use [multifactor authentication] or [network level authentication] and use strong, randomized, just-in-time local admin passwords;

Apply principle of least-privilege

- Monitor for adversarial activities
- Hunt for brute force attempts
- Monitor for cleanup of Event Logs
- Analyze logon events;

Harden infrastructure

- Use Windows Defender Firewall
- Enable tamper protection
- Enable cloud-delivered protection
- Turn on attack surface reduction rules and [Antimalware Scan Interface] for Office [Visual Basic for Applications].¹⁰

41. Given that Defendant was storing the PII of Plaintiff and Class Members, Defendant could and should have implemented all of the above measures to prevent and detect cyber-attacks.

42. The occurrence of the Data Breach indicates that Defendant failed to adequately implement one or more of the above measures to prevent ransomware attacks, resulting in the Data

¹⁰ See Human-operated ransomware attacks: A preventable disaster (Mar 5, 2020), available at: <https://www.microsoft.com/security/blog/2020/03/05/human-operated-ransomware-attacks-a-preventable-disaster/> (last visited Nov. 11, 2021).

Breach and the exposure of the PII of an undisclosed amount of current and former consumers and employees, including Plaintiff and Class Members.

Defendant Acquires, Collects, and Stores the PII of Plaintiff and Class Members

43. Defendant has historically acquired, collected, and stored the PII of Plaintiff and Class Members.

44. As part of being a customer and/or employee of Defendant, Plaintiff and Class Members, are required to give their sensitive and confidential PII to Defendant. Defendant retains and stores this information, and derives a substantial economic benefit from the PII that it collects. But for the collection of Plaintiff's and Class Members' PII, Defendant would be unable to sell or manufacture automobile parts or employ anyone for the purpose of assisting Defendant with manufacturing car components.

45. By obtaining, collecting, and storing the PII of Plaintiff and Class Members, Defendant assumed legal and equitable duties and knew or should have known that it was responsible for protecting the PII from disclosure.

46. Plaintiff and Class Members have taken reasonable steps to maintain the confidentiality of their PII and relied on Defendant to keep their PII confidential and maintained securely, to use this information for business purposes only, and to make only authorized disclosures of this information.

47. Defendant could have prevented this Data Breach by properly securing and encrypting the files and file servers containing the PII of Plaintiff and Class Members.

48. Defendant's policies on its website include promises and legal obligations to maintain and protect PII, demonstrating an understanding of the importance of securing PII.¹¹

¹¹ <https://www.tiw.co.jp/en/privacy>

49. Defendant’s negligence in safeguarding the PII of Plaintiff and Class Members is exacerbated by the repeated warnings and alerts directed to protecting and securing sensitive data.

50. Despite the prevalence of public announcements of data breach and data security compromises, Defendant failed to take appropriate steps to protect the PII of Plaintiff and Class Members from being compromised.

Defendant Knew or Should Have Known of the Risk Because the Manufacturing Sector is Particularly Susceptible to Cyber Attacks

51. Defendant knew and understood unprotected or exposed PII in the custody of manufacturing companies, such as Defendant, is valuable and highly sought after by nefarious third parties seeking to illegally monetize that PII through unauthorized access, as these companies maintain highly sensitive PII of employees and consumers, including Social Security numbers and financial information.

Value of Personally Identifiable Information

52. The Federal Trade Commission (“FTC”) defines identity theft as “a fraud committed or attempted using the identifying information of another person without authority.”¹² The FTC describes “identifying information” as “any name or number that may be used, alone or in conjunction with any other information, to identify a specific person,” including, among other things, “[n]ame, Social Security number, date of birth, official State or government issued driver’s license or identification number, alien registration number, government passport number, employer or taxpayer identification number.”¹³

53. The PII of individuals remains of high value to criminals, as evidenced by the prices the criminals will pay through the dark web. Numerous sources cite dark web pricing for stolen

¹² 17 C.F.R. § 248.201 (2013).

¹³ *Id.*

identity credentials. For example, Personal Information can be sold at a price ranging from \$40 to \$200, and bank details have a price range of \$50 to \$200.¹⁴ Experian reports that a stolen credit or debit card number can sell for \$5 to \$110 on the dark web.¹⁵ Criminals can also purchase access to entire company data breaches from \$900 to \$4,500.¹⁶

54. Social Security numbers, for example, are among the worst kind of PII to have stolen because they may be put to a variety of fraudulent uses and are difficult for an individual to change. The Social Security Administration stresses that the loss of an individual's Social Security number, as is the case here, can lead to identity theft and extensive financial fraud:

A dishonest person who has your Social Security number can use it to get other personal information about you. Identity thieves can use your number and your good credit to apply for more credit in your name. Then, they use the credit cards and don't pay the bills, it damages your credit. You may not find out that someone is using your number until you're turned down for credit, or you begin to get calls from unknown creditors demanding payment for items you never bought. Someone illegally using your Social Security number and assuming your identity can cause a lot of problems.¹⁷

55. What is more, it is no easy task to change or cancel a stolen Social Security number. An individual cannot obtain a new Social Security number without significant paperwork and evidence of actual misuse. In other words, preventive action to defend against the possibility of misuse of a Social Security number is not permitted; an individual must show evidence of actual, ongoing fraud activity to obtain a new number.

¹⁴ *Your personal data is for sale on the dark web. Here's how much it costs*, Digital Trends, Oct. 16, 2019, available at: <https://www.digitaltrends.com/computing/personal-data-sold-on-the-dark-web-how-much-it-costs/> (last visited Jan. 19, 2022).

¹⁵ *Here's How Much Your Personal Information Is Selling for on the Dark Web*, Experian, Dec. 6, 2017, available at: <https://www.experian.com/blogs/ask-experian/heres-how-much-your-personal-information-is-selling-for-on-the-dark-web/> (last visited Jan 19, 2022).

¹⁶ *In the Dark*, VPNOverview, 2019, available at: <https://vpnoverview.com/privacy/anonymous-browsing/in-the-dark/> (last visited Jan. 19, 2022).

¹⁷ Social Security Administration, *Identity Theft and Your Social Security Number*, available at: <https://www.ssa.gov/pubs/EN-05-10064.pdf> (last visited Jan. 19, 2022).

56. Even then, a new Social Security number may not be effective. According to Julie Ferguson of the Identity Theft Resource Center, “[t]he credit bureaus and banks are able to link the new number very quickly to the old number, so all of that old bad information is quickly inherited into the new Social Security number.”¹⁸

57. Based on the foregoing, the information compromised in the Data Breach is significantly more valuable than the loss of, for example, credit card information in a retailer data breach because, there, victims can cancel or close credit and debit card accounts. The information compromised in this Data Breach is impossible to “close” and difficult, if not impossible, to change—one’s Social Security number.

58. This data demands a much higher price on the black market. Martin Walter, senior director at cybersecurity firm RedSeal, explained, “Compared to credit card information, personally identifiable information and Social Security numbers are worth more than 10x on the black market.”¹⁹

59. Among other forms of fraud, identity thieves may use Social Security numbers to obtain driver’s licenses, government benefits, medical services, and housing or even give false information to police.

60. The fraudulent activity resulting from the Data Breach may not come to light for years.

61. There may be a time lag between when harm occurs versus when it is discovered, and also between when PII is stolen and when it is used. According to the U.S. Government

¹⁸ Bryan Naylor, *Victims of Social Security Number Theft Find It’s Hard to Bounce Back*, NPR (Feb. 9, 2015), available at: <http://www.npr.org/2015/02/09/384875839/data-stolen-by-anthem-s-hackers-has-millions-worrying-about-identity-theft> (last visited Jan. 19, 2022).

¹⁹ Time Greene, *Anthem Hack: Personal Data Stolen Sells for 10x Price of Stolen Credit Card Numbers*, IT World, (Feb. 6, 2015), available at: <https://www.networkworld.com/article/2880366/anthem-hack-personal-data-stolen-sells-for-10x-price-of-stolen-credit-card-numbers.html> (last visited Nov. 11, 2021).

Accountability Office (“GAO”), which conducted a study regarding data breaches:

[L]aw enforcement officials told us that in some cases, stolen data may be held for up to a year or more before being used to commit identity theft. Further, once stolen data have been sold or posted on the Web, fraudulent use of that information may continue for years. As a result, studies that attempt to measure the harm resulting from data breaches cannot necessarily rule out all future harm.²⁰

62. At all relevant times, Defendant knew, or reasonably should have known, of the importance of safeguarding the PII of Plaintiff and Class Members, including Social Security numbers, and of the foreseeable consequences that would occur if Defendant’s data security system and network was breached, including, specifically, the significant costs that would be imposed on Plaintiff and Class Members as a result of a breach.

63. Plaintiff and Class Members now face years of constant surveillance of their financial and personal records, monitoring, and loss of rights. The Class is incurring and will continue to incur such damages in addition to any fraudulent use of their PII.

64. Defendant was, or should have been, fully aware of the unique type and the significant volume of data on Defendant’s server(s), amounting to potentially thousands of individuals’ detailed PII, and, thus, the significant number of individuals who would be harmed by the exposure of the unencrypted data.

65. In the breach notification letter, Defendant made an offer of twelve (12) months of credit and identity monitoring services. This is wholly inadequate to compensate Plaintiff and Class Members as it fails to provide for the fact that victims of data breaches and other unauthorized disclosures commonly face multiple years of ongoing identity theft and financial fraud, and it entirely fails to provide sufficient compensation for the unauthorized release and

²⁰ Report to Congressional Requesters, GAO, at 29 (June 2007), available at: <https://www.gao.gov/assets/gao-07-737.pdf> (last visited Jan. 19, 2022).

disclosure of Plaintiff's and Class Members' PII.

66. The injuries to Plaintiff and Class Members were directly and proximately caused by Defendant's failure to implement or maintain adequate data security measures for the PII of Plaintiff and Class Members.

67. The ramifications of Defendant's failure to keep secure the PII of Plaintiff and Class Members are long lasting and severe. Once PII is stolen, particularly Social Security numbers, fraudulent use of that information and damage to victims may continue for years.

Defendant Violated the FTC Act

68. Section 5 of the FTC Act, 15 U.S.C. § 45, prohibits "unfair . . . practices in or affecting commerce," including, as interpreted and enforced by the FTC, the unfair act or practice by businesses, such as Defendant, of failing to use reasonable measures to protect PII. The FTC publications and orders described above also form part of the basis of Defendant's duty in this regard.

69. Defendant violated Section 5 of the FTC Act by failing to use reasonable measures to protect PII and not complying with applicable industry standards, as described in detail herein. Defendant's conduct was particularly unreasonable given the nature and amount of PII it obtained and stored and the foreseeable consequences of the immense damages that would result to Plaintiff and the Nationwide Class.

Plaintiff Jonathan Phelps's Experience

70. Plaintiff was required to provide and did provide his PII to Defendant during the course of his employment with Defendant. The PII included his name, address, date of birth, Social Security Numbers, driver's license number, telephone number, and other financial and tax information.

71. To date, Toyotetsu has done next to nothing to adequately protect Plaintiff and Class Members, or to compensate them for their injuries sustained in this Data Breach.

72. Defendant's data breach notice letter downplays the theft of Plaintiff's and Class Members PII, when the facts demonstrate that the PII was targeted, accessed, and exfiltrated in a criminal cyberattack. The fraud and identity monitoring services offered by Defendant are only for one year, and it places the burden squarely on Plaintiff and Class Members by requiring them to expend time signing up for the service and addressing timely issues.

73. Plaintiff and Class Members have been further damaged by the compromise of their PII.

74. Plaintiff Phelps's PII was compromised in the Data Breach, and was likely stolen and in the hands of cybercriminals who illegally accessed Toyotetsu's network for the specific purpose of targeting the PII.

75. Plaintiff Phelps typically takes measures to protect his PII, and is very careful about sharing his PII. Phelps has never knowingly transmitted unencrypted PII over the internet or other unsecured source.

76. Plaintiff Phelps stores any documents containing his PII in a safe and secure location, and he diligently chooses unique usernames and passwords for his online accounts.

77. As a result of the Data Breach, Plaintiff has suffered a loss of time and has spent and continues to spend a considerable amount of time on issues related to this Data Breach. He monitors accounts and credit scores and has sustained emotional distress. This is time that was lost and unproductive and took away from other activities and duties.

78. Plaintiff has recently experienced fraudulent charges on a credit card account to which he is an authorized user, totaling approximately \$300.00.

79. Plaintiff also suffered actual injury in the form of damages to and diminution in the value of his PII—a form of intangible property that he entrusted to Defendant for the purpose of obtaining employment from Defendant, which was compromised in and as a result of the Data Breach.

80. Plaintiff suffered lost time, annoyance, interference, and inconvenience as a result of the Data Breach and has anxiety and increased concerns for the loss of his privacy.

81. Plaintiff has suffered imminent and impending injury arising from the substantially increased risk of fraud, identity theft, and misuse resulting from his PII, especially his Social Security Number, being placed in the hands of criminals.

82. Defendant obtained and continues to maintain Plaintiff's PII and has a continuing legal duty and obligation to protect that PII from unauthorized access and disclosure. Defendant required the PII from Plaintiff when he began employment with Defendant. Plaintiff, however, would not have entrusted his PII to Defendant had he known that it would fail to maintain adequate data security. Plaintiff's PII was compromised and disclosed as a result of the Data Breach.

83. As a result of the Data Breach, Plaintiff anticipates spending considerable time and money on an ongoing basis to try to mitigate and address harms caused by the Data Breach. As a result of the Data Breach, Plaintiff is at a present risk and will continue to be at increased risk of identity theft and fraud for years to come.

CLASS ALLEGATIONS

84. Plaintiff brings this suit on behalf of himself and a class of similarly situated individuals under Kentucky Rule of Civil Procedure 23.01, *et seq.*, which is preliminarily defined as:

All persons Toyotetsu North America identified as being among those individuals impacted by the Data Breach, including all who were sent a notice

of the Data Breach.

85. Excluded from the Classes are the following individuals and/or entities: Defendant and Defendant's parents, subsidiaries, affiliates, officers and directors, and any entity in which Defendant has a controlling interest; all individuals who make a timely election to be excluded from this proceeding using the correct protocol for opting out; and all judges assigned to hear any aspect of this litigation, as well as their immediate family members.

86. **Numerosity.** The Class Members are so numerous that joinder of all members is impracticable. Though the exact number and identities of Class Members are unknown at this time, reports indicate that approximately 12,450 individuals had their PII compromised in this Data Breach. The identities of Class Members are ascertainable through Toyotetsu's records, Class Members' records, publication notice, self-identification, and other means.

87. **Commonality.** There are questions of law and fact common to the Class, which predominate over any questions affecting only individual Class Members. These common questions of law and fact include, without limitation:

- a. Whether Toyotetsu unlawfully used, maintained, lost, or disclosed Plaintiff's and Class Members' PII;
- b. Whether Toyotetsu failed to implement and maintain reasonable security procedures and practices appropriate to the nature and scope of the information compromised in the Data Breach;
- c. Whether Toyotetsu data security systems prior to and during the Data Breach complied with applicable data security laws and regulations;
- d. Whether Toyotetsu data security systems prior to and during the Data Breach were consistent with industry standards;

- e. Whether Toyotetsu owed a duty to Class Members to safeguard their PII;
- f. Whether Toyotetsu breached its duty to Class Members to safeguard their PII;
- g. Whether computer hackers obtained Class Members' PII in the Data Breach;
- h. Whether Toyotetsu knew or should have known that its data security systems and monitoring processes were deficient;
- i. Whether Plaintiff and Class Members suffered legally cognizable damages as a result of Toyotetsu's misconduct;
- j. Whether Toyotetsu's conduct was negligent;
- k. Whether Toyotetsu's conduct was *per se* negligent, and;
- l. Whether Plaintiff and Class Members are entitled to damages, civil penalties, punitive damages, and/or injunctive relief.

88. **Typicality.** Plaintiff's claims are typical of those of other Class Members because Plaintiff's PII, like that of every other Class member, was compromised in the Data Breach.

89. **Adequacy of Representation.** Plaintiff will fairly and adequately represent and protect the interests of the Members of the Class. Plaintiff's Counsel is competent and experienced in litigating Class actions, including data privacy litigation of this kind.

90. **Predominance.** Toyotetsu has engaged in a common course of conduct toward Plaintiff and Class Members, in that all the Plaintiff's and Class Members' data was stored on the same computer systems and unlawfully accessed in the same way. The common issues arising from Defendant's conduct affecting Class Members set out above predominate over any individualized issues. Adjudication of these common issues in a single action has important and desirable advantages of judicial economy.

91. **Superiority.** A Class action is superior to other available methods for the fair and

efficient adjudication of the controversy. Class treatment of common questions of law and fact is superior to multiple individual actions or piecemeal litigation. Absent a Class action, most Class Members would likely find that the cost of litigating their individual claims is prohibitively high and would therefore have no effective remedy. The prosecution of separate actions by individual Class Members would create a risk of inconsistent or varying adjudications with respect to individual Class Members, which would establish incompatible standards of conduct for Toyotetsu. In contrast, the conduct of this action as a Class action presents far fewer management difficulties, conserves judicial resources and the parties' resources, and protects the rights of each Class member.

92. Toyotetsu has acted on grounds that apply generally to the Class as a whole, so that Class certification, injunctive relief, and corresponding declaratory relief are appropriate on a Class-wide basis.

93. Likewise, particular issues are appropriate for certification because such claims present only particular, common issues, the resolution of which would advance the disposition of this matter and the parties' interests therein. Such particular issues include, but are not limited to:

- m. Whether Toyotetsu owed a legal duty to Plaintiff and the Class to exercise due care in collecting, storing, and safeguarding their PII;
- n. Whether Toyotetsu's security measures to protect its data systems were reasonable in light of best practices recommended by data security experts;
- o. Whether Toyotetsu's failure to institute adequate protective security measures amounted to negligence;
- p. Whether Toyotetsu failed to take commercially reasonable steps to safeguard employee and consumer PII; and

q. Whether adherence to FTC data security recommendations, and measures recommended by data security experts would have reasonably prevented the data breach.

94. Finally, all members of the proposed Class are readily ascertainable. Toyotetsu has access to Class Members' names and addresses affected by the Data Breach. Class Members have already been preliminarily identified and sent notice of the Data Breach by Toyotetsu.

FIRST CAUSE OF ACTION
NEGLIGENCE
(On Behalf of Plaintiff and the Class)

95. Plaintiff incorporates by reference all other allegations in the Complaint as if fully set forth herein.

96. Toyotetsu knowingly collected, came into possession of, and maintained Plaintiff's and Class Members' PII, and had a duty to exercise reasonable care in safeguarding, securing, and protecting such information from being compromised, lost, stolen, misused, and/or disclosed to unauthorized parties.

97. Toyotetsu had a duty under common law to have procedures in place to detect and prevent the loss or unauthorized dissemination of Plaintiff's and Class Members' PII.

98. Defendant had full knowledge of the sensitivity of the PII and the types of harm that Plaintiff and Class Members could and would suffer if the PII were wrongfully disclosed.

99. By assuming the responsibility to collect and store this data, and in fact doing so, and sharing it and using it for commercial gain, Defendant had a duty of care to use reasonable means to secure and safeguard its computer property—and Class Members' PII held within it—to prevent disclosure of the information, and to safeguard the information from theft. Defendant's duty included a responsibility to implement processes by which they could detect a breach of its

security systems in a reasonably expeditious period of time and to give prompt notice to those affected in the case of a data breach.

100. Toyotetsu had a duty to employ reasonable security measures under Section 5 of the Federal Trade Commission Act, 15 U.S.C. § 45, which prohibits “unfair. . . practices in or affecting commerce,” including, as interpreted and enforced by the FTC, the unfair practice of failing to use reasonable measures to protect confidential data.

101. Toyotetsu had a duty to employ reasonable security measures and otherwise protect the PII of Plaintiff and Class Members pursuant to in K.R.S. § 365.720 - § 365.732.

102. Toyotetsu, through its actions and/or omissions, unlawfully breached its duty to Plaintiff and Class members by failing to exercise reasonable care in protecting and safeguarding Plaintiff’s and Class Members’ PII within Toyotetsu’s possession.

103. Toyotetsu, through its actions and/or omissions, unlawfully breached its duty to Plaintiff and Class members by failing to have appropriate procedures in place to detect and prevent dissemination of Plaintiff’s and Class Members’ PII.

104. Toyotetsu, through its actions and/or omissions, unlawfully breached its duty to timely disclose to Plaintiff and Class Members that the PII within Toyotetsu s’ possession might have been compromised and precisely the type of information compromised.

105. Toyotetsu’s breach of duties owed to Plaintiff and Class Members caused Plaintiff’s and Class Members’ PII to be compromised.

106. As a result of Toyotetsu’s ongoing failure to notify Plaintiff and Class Members regarding the type of PII has been compromised, Plaintiff and Class Members are unable to take the necessary precautions to mitigate damages by preventing future fraud.

107. Toyotetsu's breaches of duty caused Plaintiff and Class Members to suffer from identity theft, loss of time and money to monitor their finances for fraud, and loss of control over their PII.

108. As a result of Toyotetsu's negligence and breach of duties, Plaintiff and Class Members are in danger of imminent harm in that their PII, which is still in the possession of third parties, will be used for fraudulent purposes.

109. Plaintiff seeks the award of actual damages on behalf of himself and the Class.

110. In failing to secure Plaintiff's and Class Members' PII and promptly notifying them of the Data Breach, Toyotetsu is guilty of oppression, fraud, or malice, in that Toyotetsu acted or failed to act with a willful and conscious disregard of Plaintiff's and Class Members' rights. Plaintiff, therefore, in addition to seeking actual damages, seeks punitive damages on behalf of himself and the Class.

111. Plaintiff seeks injunctive relief on behalf of the Class in the form of an order compelling Toyotetsu to institute appropriate data collection and safeguarding methods and policies with regard to patient information.

SECOND CAUSE OF ACTION
BREACH OF IMPLIED CONTRACT
(On Behalf of Plaintiff and the Class)

112. Plaintiff incorporates by reference all other allegations in the Complaint as if fully set forth herein.

113. Plaintiff and Class Members were required to provide their PII to Defendant as a condition of employment or use of Defendant's services.

114. Plaintiff and Class Members disclosed their PII in exchange for employment, along with Defendant's promise to protect their PII from unauthorized disclosure.

115. In its written privacy policies, Defendant Toyotetsu expressly promised Plaintiff and Class Members that it would only disclose PII under certain circumstances, none of which relate to the Data Breach.

116. Defendant further promised to comply with industry standards and to make sure that Plaintiff's and Class Members' PII would remain protected.

117. There was a meeting of the minds and an implied contractual agreement between Plaintiff and Class Members and the Defendant, under which Plaintiff and Class Members would provide their PII in exchange for Defendant's obligations to: (a) use such PII for business purposes only, (b) take reasonable steps to safeguard that PII, (c) prevent unauthorized disclosures of the PII, (d) provide Plaintiff and Class Members with prompt and sufficient notice of any and all unauthorized access and/or theft of their PII, (e) reasonably safeguard and protect the PII of Plaintiff and Class Members from unauthorized disclosure or uses, (f) retain the PII only under conditions that kept such information secure and confidential.

118. When Plaintiff and Class Members provided their PII to Defendant Toyotetsu as a condition of obtaining Toyotetsu employment, or as a condition precedent to receiving Toyotetsu services, they entered into implied contracts with Defendant pursuant to which Defendant agreed to reasonably protect such information.

119. Defendant solicited, invited, and then required Class Members to provide their PII as part of Defendant's regular business practices. Plaintiff and Class Members accepted Defendant's offers and provided their PII to Defendant.

120. In entering into such implied contracts, Plaintiff and Class Members reasonably believed and expected that Defendant's data security practices complied with relevant laws and regulations and were consistent with industry standards.

121. Plaintiff and Class Members would not have entrusted their PII to Defendant in the absence of the implied contract between them and Defendant to keep their information reasonably secure. Plaintiff and Class Members would not have entrusted their PII to Defendant in the absence of its implied promise to monitor its computer systems and networks to ensure that it adopted reasonable data security measures.

122. Plaintiff and Class Members fully and adequately performed their obligations under the implied contracts with Defendant.

123. Defendant breached its implied contracts with Class Members by failing to safeguard and protect their PII.

124. As a direct and proximate result of Defendant breaches of the implied contracts, Class Members sustained damages as alleged herein.

125. Plaintiff and Class Members are entitled to compensatory and consequential damages suffered as a result of the Data Breach.

126. Plaintiff and Class Members are also entitled to injunctive relief requiring Defendant to, e.g., (i) strengthen its data security systems and monitoring procedures; (ii) submit to future annual audits of those systems and monitoring procedures; and (iii) immediately provide adequate credit monitoring to all Class Members.

THIRD CAUSE OF ACTION
UNJUST ENRICHMENT
(On Behalf of Plaintiff and the Class)

127. Plaintiff incorporates by reference all other allegations in the Complaint as if fully set forth herein.

128. This claim is plead in the alternative to the Second Cause of Action for breach of implied contract.

129. Defendant benefited from receiving Plaintiff's and Class Members' PII by its ability to retain and use that information for its own benefit. Defendant understood this benefit.

130. Defendant also understood and appreciated that Plaintiff's and Class Members' PII was private and confidential, and its value depended upon Defendant maintaining the privacy and confidentiality of that information.

131. Plaintiff and Class Members conferred a monetary benefit upon Defendant in the form of purchasing services from Defendant, and in connection thereto, by providing their PII to Defendant with the understanding that Defendant would pay for the administrative costs of reasonable data privacy and security practices and procedures. Specifically, they were required to provide Defendant with their PII. In exchange, Plaintiff and Class members should have received adequate protection and data security for such PII held by Defendant.

132. Defendant knew Plaintiff and Class members conferred a benefit which Defendant accepted. Defendant profited from these transactions and used the PII of Plaintiff and Class Members for business purposes.

133. Defendant failed to provide reasonable security, safeguards, and protections to the PII of Plaintiff and Class Members.

134. Under the principles of equity and good conscience, Defendant should not be permitted to retain money belonging to Plaintiff and Class Members, because Defendant failed to implement appropriate data management and security measures mandated by industry standards.

135. Defendant wrongfully accepted and retained these benefits to the detriment of Plaintiff and Class Members.

136. Defendant's enrichment at the expense of Plaintiff and Class Members is and was unjust.

137. As a result of Defendant’s wrongful conduct, as alleged above, Plaintiff and the Class Members are entitled to restitution and disgorgement of all profits, benefits, and other compensation obtained by Defendant, plus attorneys’ fees, costs, and interest thereon.

FOURTH CAUSE OF ACTION
NEGLIGENCE *PER SE*
(On Behalf of Plaintiff and the Class)

138. Plaintiff incorporates by reference all other allegations in the Complaint as if fully set forth herein.

139. Section 5 of the FTC Act, 15 U.S.C. § 45, prohibits “unfair . . . practices in or affecting commerce” including, as interpreted and enforced by the FTC, the unfair act or practice by Defendant of failing to use reasonable measures to protect PII. Various FTC publications and orders also form the basis of Defendant’s duty.

140. Defendant violated Section 5 of the FTC Act (and similar state statutes) by failing to use reasonable measures to protect PII and not complying with industry standards. Defendant’s conduct was particularly unreasonable given the nature and amount of PII obtained and stored and the foreseeable consequences of a data breach on Defendant’s systems.

141. Defendant’s violation of Section 5 of the FTC Act (and similar state statutes) constitutes negligence per se.

142. The harm that has occurred is the type of harm the FTC Act (and similar state statutes) was intended to guard against. Indeed, the FTC has pursued over fifty enforcement actions against businesses which, as a result of their failure to employ reasonable data security measures and avoid unfair and deceptive practices, caused the same harm suffered by Plaintiff and Class Members.

143. As a direct and proximate result of Defendant Toyotetsu’s negligence, Plaintiff and Class Members have been injured and are 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 their 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 their bargains and overcharges for services; and other economic and non-economic harm.

PRAYER FOR RELIEF

WHEREFORE, Plaintiff, on behalf of himself and Class Members, request judgment against Defendant and that the Court grant the following:

- A. For an order certifying the Class, as defined herein, and appointing Plaintiff and his Counsel to represent each such Class;
- B. For equitable relief enjoining Defendant from engaging in the wrongful conduct complained of herein pertaining to the misuse and/or disclosure of the PII of Plaintiff and Class Members, and from refusing to issue prompt, complete, any accurate disclosures to Plaintiff and Class Members;
- C. For injunctive relief requested by Plaintiff, including but not limited to, injunctive and other equitable relief as is necessary to protect the interests of Plaintiff and Class Members, including but not limited to an order:
 - i. prohibiting Defendant from engaging in the wrongful and unlawful acts

described herein;

- ii. requiring Defendant to protect, including through encryption, all data collected through the course of its business in accordance with all applicable regulations, industry standards, and federal, state, or local laws;
- iii. requiring Defendant to delete, destroy, and purge the personal identifying information of Plaintiff and Class Members unless Defendant can provide to the Court reasonable justification for the retention and use of such information when weighed against the privacy interests of Plaintiff and Class Members;
- iv. requiring Defendant to implement and maintain a comprehensive Information Security Program designed to protect the confidentiality and integrity of the PII of Plaintiff and Class Members;
- v. prohibiting Defendant from maintaining the PII of Plaintiff and Class Members on a cloud-based database;
- vi. requiring Defendant to engage independent third-party security auditors/penetration testers as well as internal security personnel to conduct testing, including simulated attacks, penetration tests, and audits on Defendant's systems on a periodic basis, and ordering Defendant to promptly correct any problems or issues detected by such third-party security auditors;
- vii. requiring Defendant to engage independent third-party security auditors and internal personnel to run automated security monitoring;
- viii. requiring Defendant to audit, test, and train its security personnel regarding any new or modified procedures;
- ix. requiring Defendant to segment data by, among other things, creating firewalls

and access controls so that if one area of Defendant's network is compromised, hackers cannot gain access to other portions of Defendant's systems;

- x. requiring Defendant to conduct regular database scanning and securing checks;
- xi. requiring Defendant to establish an information security training program that includes at least annual information security training for all employees, with additional training to be provided as appropriate based upon the employees' respective responsibilities with handling personal identifying information, as well as protecting the personal identifying information of Plaintiff and Class Members;
- xii. requiring Defendant to conduct internal training and education routinely and continually, and on an annual basis to inform internal security personnel how to identify and contain a breach when it occurs and what to do in response to a breach;
- xiii. requiring Defendant to implement a system of tests to assess its employees' knowledge of the education programs discussed in the preceding subparagraphs, as well as randomly and periodically testing employees' compliance with Defendant's policies, programs, and systems for protecting personal identifying information;
- xiv. requiring Defendant to implement, maintain, regularly review, and revise as necessary a threat management program designed to appropriately monitor Defendant's information networks for threats, both internal and external, and assess whether monitoring tools are appropriately configured, tested, and updated;

- xv. requiring Defendant to meaningfully educate all Class Members about the threats that they face as a result of the loss of their confidential PII to third parties, as well as the steps affected individuals must take to protect themselves;
- xvi. requiring Defendant to implement logging and monitoring programs sufficient to track traffic to and from Defendant’s servers; and for a period of 10 years, appointing a qualified and independent third-party assessor to conduct a SOC 2 Type 2 attestation on an annual basis to evaluate Defendant’s compliance with the terms of the Court’s final judgment, to provide such report to the Court and to counsel for the class, and to report any deficiencies with compliance of the Court’s final judgment;
- D. For an award of damages, including actual, statutory, nominal, and consequential damages, as allowed by law in an amount to be determined;
- E. For an award of attorneys’ fees, costs, and litigation expenses, as allowed by law;
- F. For prejudgment interest on all amounts awarded; and
- G. Such other and further relief as this Court may deem just and proper.

DEMAND FOR JURY TRIAL

Plaintiff hereby demands that this matter be tried before a jury.

Respectfully submitted,

Terence R. Coates (*pro hac vice* forthcoming)
MARKOVITS, STOCK & DEMARCO, LLC
 3825 Edwards Road, Suite 650
 Cincinnati, OH 45209
 Phone: (513) 651-3700
 Fax: (513) 665-0219
tcoates@msdlegal.com
Counsel for Plaintiff and the Class

and

Joseph B. Venters
VENTERS LAW OFFICE
 P.O. Box 1749
 Somerset, KY 42502
 Phone: (606) 451-0332
 Fax: (606) 451-0335
joey@venterslaw.com
Co-Counsel for Plaintiff and the Class

B706A0DB-C743-40C4-BF79-031EC380ED41 : 000033 of 000036

Presiding Judge: HON. JOHN G. PRATHER JR. (628416)

COM : 000033 of 000033

COMMONWEALTH OF KENTUCKY
28th JUDICIAL CIRCUIT
PULASKI CIRCUIT COURT
CIVIL ACTION NO. 22-CI-00328

JONATHAN PHELPS

PLAINTIFF

V.

TOYOTETSU NORTH AMERICA

DEFENDANT

AGREED ORDER

Plaintiff Jonathan Phelps together with Defendant Toyotetsu North America, through counsel, do stipulate and agree that Defendant Toyotetsu North America. may have up to and including May 31, 2022 within which to file a responsive pleading to Plaintiff’s Complaint.

Accordingly, it is SO ORDERED this ____ day of _____, 2022.

Judge, John G. Prather, Jr.

Order prepared by counsel for Defendant Toyotetsu North America.

Having seen and agreed:

/s/ Joseph B. Venters (via email 5-4-22)

Joseph B. Venters
VENTERS LAW OFFICE
P.O. Box 1749
Somerset, KY 42502
606-451-0332
606-451-0335
joey@venterslaw.com

Terence R. Coates
MARKOVITIS, STOCK & DEMARCO, LLC
3825 Edwards Road, Suite 650
Cincinnati, OH 45209
513-651-3700
513-665-0219 (Fax)
tcoates@msdlegal.com

Attorneys for Plaintiff and the Class

/s/ Judd R. Uhl

Judd R. Uhl (89578)
R. Morgan Salisbury (94922)
LEWIS, BRISBOIS, BISGAARD & SMITH
250 E. Fifth Street, Suite 2000
Cincinnati, OH 45202
judd.uhl@lewisbrisbois.com
morgan.salisbury@lewisbrisbois.com
(513) 08-9911/(513) 808-9912 (Fax)

*Attorneys for Defendant
Toyotetsu North America*

CLERK'S CERTIFICATE OF SERVICE

I certify that on _____, 2022, the foregoing was sent to the following parties/counsel of record:

Terence R. Coates
MARKOVITIS, STOCK & DEMARCO, LLC
3825 Edwards Road, Suite 650
Cincinnati, OH 45209
513-651-3700
513-665-0219 (Fax)
tcoates@msdlegal.com

Joseph B. Venters
VENTERS LAW OFFICE
P.O. Box 1749
Somerset, KY 42502
606-451-0332
606-451-0335
joey@venterslaw.com
Attorneys for Plaintiff and the Class

Judd R. Uhl
R. Morgan Salisbury
LEWIS, BRISBOIS, BISGAARD & SMITH
250 E. Fifth Street, Suite 2000
Cincinnati, OH 45202
judd.uhl@lewisbrisbois.com
morgan.salisbury@lewisbrisbois.com
(513) 08-9911/(513) 808-9912 (Fax)
Attorneys for Defendant
Toyotetsu North America

Clerk / Deputy Clerk

**COMMONWEALTH OF KENTUCKY
28th JUDICIAL CIRCUIT
PULASKI CIRCUIT COURT
CIVIL ACTION NO. 22-CI-00328**

JONATHAN PHELPS

PLAINTIFF

V.

TOYOTETSU NORTH AMERICA

DEFENDANT

NOTICE OF APPEARANCE AND ELECTION TO RECEIVE ELECTRONIC SERVICE

Come now Judd R. Uhl and R. Morgan Salisbury of the law office of Lewis Brisbois Bisgaard & Smith LLP and hereby gives notice of their appearance as Counsel of record for Defendant Toyotetsu North America.

Undersigned counsel gives notice of their election under CR 5.02(2) to receive service electronically. Counsel elects to serve and receive pleadings by email at the following email addresses:

- judd.uhl@lewisbrisbois.com;
- morgan.salisbury@lewisbrisbois.com
- mindy.stallmeyer@lewisbrisbois.com

In accordance with CR 5.02(2), documents to be filed with the clerk should now be electronically served on or before the day of filing to the above email addresses.

/s/ Judd R. Uhl
Judd R. Uhl (89578)
R. Morgan Salisbury (94922)
LEWIS, BRISBOIS, BISGAARD & SMITH
250 E. Fifth Street, Suite 2000
Cincinnati, OH 45202
judd.uhl@lewisbrisbois.com
morgan.salisbury@lewisbrisbois.com
(513) 08-9911/(513) 808-9912 (Fax)
*Attorneys for Defendant
Toyotetsu North America*

EA : 000001 of 000002

CERTIFICATE OF SERVICE

I certify that on May 4, 2022, the foregoing was sent to the following counsel of record via email:

Terence R. Coates
MARKOVITIS, STOCK & DEMARCO, LLC
3825 Edwards Road, Suite 650
Cincinnati, OH 45209
513-651-3700
513-665-0219 (Fax)
tcoates@msdlegal.com

Joseph B. Venters
VENTERS LAW OFFICE
P.O. Box 1749
Somerset, KY 42502
606-451-0332
606-451-0335
joey@venterslaw.com
Attorneys for Plaintiff and the Class

/s/ Judd R. Uhl
Judd R. Uhl (89578)
R. Morgan Salisbury (94922)

COMMONWEALTH OF KENTUCKY
28th JUDICIAL CIRCUIT
PULASKI CIRCUIT COURT
CIVIL ACTION NO. 22-CI-00328

ENTERED
EJYH-SCC
MAY - 6 2022
PULASKI CIRC. DIST COURT
BY VP PLAINTIFF D.C.

JONATHAN PHELPS

V.

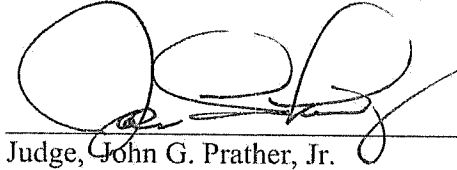
TOYOTETSU NORTH AMERICA

DEFENDANT

AGREED ORDER

Plaintiff Jonathan Phelps together with Defendant Toyotetsu North America, through counsel, do stipulate and agree that Defendant Toyotetsu North America. may have up to and including May 31, 2022 within which to file a responsive pleading to Plaintiff's Complaint.

Accordingly, it is SO ORDERED this 5th day of May, 2022.



Judge, John G. Prather, Jr.

Order prepared by counsel for Defendant Toyotetsu North America.

Having seen and agreed:

/s/ Joseph B. Venters (via email 5-4-22)

Joseph B. Venters
VENTERS LAW OFFICE
P.O. Box 1749
Somerset, KY 42502
606-451-0332
606-451-0335
joey@venterslaw.com

Terence R. Coates
MARKOVITIS, STOCK & DEMARCO, LLC
3825 Edwards Road, Suite 650
Cincinnati, OH 45209
513-651-3700
513-665-0219 (Fax)
tcoates@msdlegal.com
Attorneys for Plaintiff and the Class

/s/ Judd R. Uhl

Judd R. Uhl (89578)
R. Morgan Salisbury (94922)
LEWIS, BRISBOIS, BISGAARD & SMITH
250 E. Fifth Street, Suite 2000
Cincinnati, OH 45202
judd.uhl@lewisbrisbois.com
morgan.salisbury@lewisbrisbois.com
(513) 08-9911/(513) 808-9912 (Fax)
*Attorneys for Defendant
Toyotetsu North America*

CLERK'S CERTIFICATE OF SERVICE

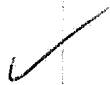
I certify that on May, 6, 2022, the foregoing was sent to the following

parties/counsel of record:

Terence R. Coates
MARKOVITIS, STOCK & DEMARCO, LLC
3825 Edwards Road, Suite 650
Cincinnati, OH 45209
513-651-3700
513-665-0219 (Fax)
tcoates@msdlegal.com



Joseph B. Venters
VENTERS LAW OFFICE
P.O. Box 1749
Somerset, KY 42502
606-451-0332
606-451-0335
joey@venterslaw.com
Attorneys for Plaintiff and the Class



Judd R. Uhl
R. Morgan Salisbury
LEWIS, BRISBOIS, BISGAARD & SMITH
250 E. Fifth Street, Suite 2000
Cincinnati, OH 45202
judd.uhl@lewisbrisbois.com
morgan.salisbury@lewisbrisbois.com
(513) 08-9911/(513) 808-9912 (Fax)
Attorneys for Defendant
Toyotetsu North America



Clerk / Deputy Clerk

**COMMONWEALTH OF KENTUCKY
28TH JUDICIAL CIRCUIT
PULASKI CIRCUIT COURT
CIVIL ACTION NO. 22-CI-00328**

**JONATHAN PHELPS, individually and on
behalf of all others similarly situated**

PLAINTIFF

v.

TOYOTETSU NORTH AMERICA

DEFENDANT

NOTICE OF REMOVAL

Please take notice that, pursuant to 28 U.S.C. §§ 1332, 1441, and 1446, Defendant Toyotetsu North America is removing this action to the United States District Court for the Eastern District of Kentucky - London Division. A copy of the Notice of Removal filed with the United States District Court is attached as Exhibit A.

Pursuant to 28 U.S.C. § 1446(d), this Court should not proceed further in this action unless and until the case is remanded.

Dated: May 13, 2022

Respectfully,

/s/ R. Morgan Salisbury
Judd R. Uhl (89578)
R. Morgan Salisbury (94922)
Lewis Brisbois Bisgaard & Smith, LLP
250 E. Fifth Street, Suite 2000
Cincinnati, OH 45202
judd.uhl@lewisbrisbois.com
morgan.salisbury@lewisbrisbois.com
Phone: (513) 808-9911
Attorneys for Toyotetsu North America

CERTIFICATE OF SERVICE

I hereby certify that on May 13, 2022, I served a copy of the foregoing via electronic filing and/or regular U.S. Mail, postage prepaid, on the following:

Terence R. Coates
MARKOVITS, STOCK & DEMARCO, LLC
3825 Edwards Road, Suite 650
Cincinnati, OH 45209
Phone: (513) 651-3700
Fax: (513) 665-0219
tcoates@msdlegal.com
Counsel for Plaintiff and the Class

Joseph B. Venters
VENTERS LAW OFFICE
P.O. Box 1749
Somerset, KY 42502
Phone: (606) 451-0332
Fax: (606) 451-0335
joey@venterslaw.com
Co-Counsel for Plaintiff and the Class

/s/ R. Morgan Salisbury
Judd R. Uhl (89578)
R. Morgan Salisbury (94922)

ClassAction.org

This complaint is part of ClassAction.org's searchable class action lawsuit database and can be found in this post: [Toyotetsu North America Facing Class Action Over October 2021 Data Breach](#)
