UNITED STATES DISTRICT COURT
SOUTHERN DISTRICT OF NEW YORK

ESSILOR INTERNATIONAL SAS and ESSILOR MANUFACTURING (THAILAND) CO., LTD., Plaintiffs, -against- J.P. MORGAN CHASE BANK, N.A., Defendant.	Index No. 22-cv-3361 **COMPLAINT** **DEMAND FOR JURY TRIAL**

Essilor International SAS ("Essilor") and Essilor Manufacturing (Thailand) Co., Ltd. ("EMTC") (Essilor and EMTC sometimes are referred to hereafter as "Plaintiffs"), by and through their attorneys, bring this action against Defendant J.P. Morgan Chase Bank, N.A. ("Defendant," or "JPM"), and allege as follows:

NATURE OF THE ACTION

1. Plaintiffs are the victims of a complex fraud orchestrated by international cybercriminals resulting in approximately $272 million of fraudulent transfers from an EMTC account maintained at a New York, NY branch of JPM (the "NY Account"). The transfers were made from mid-September 2019 until mid-December 2019.

2. Plaintiffs, through a costly and burdensome process, have been able to recover some of the fraudulently transferred funds. To date, however, Plaintiffs have been unable to recover transfers totaling approximately $100 million. The fraudulent transfers are identified in more detail in Exhibit A attached hereto.[1]

3. When JPM described its services to EMTC, and to EMTC's parent company, Essilor, JPM recited its "commitment to the delivery of the highest standard of service and support available" and promised that it would put in place a "dedicated Client Service Team" to provide "strategic focus, direction and excellence in client service and support." JPM, Essilor, and EMTC also agreed that the NY Account would be subject to a daily overdraft limit ("DOL") of $10 million.

[1] Exhibit A is based on information currently available to Plaintiffs and is not necessarily an exhaustive list of the fraudulent transfers for which JPM is liable. As set forth below, under New York law, JPM is liable for losses relating to *all* unauthorized transfers from the EMTC account regardless of whether they are listed on Exhibit A.

4. During the parties' communications, JPM emphasized its commitment to fighting global financial crimes and described applicable account controls designed to achieve that end. JPM represented that transactions would be monitored for money laundering and other suspicious activity in accordance with regulatory compliance and warned that such monitoring could delay execution. Under anti money laundering ("AML") laws and regulations, JPM was required to monitor EMTC's account activity, including any unusually large volume of transfers, and report suspicious activity. JPM was tasked with developing an effective training program and an understanding of Plaintiffs' business sufficient to assess whether transactions were suspicious, including patterns of transactions that did not fit EMTC's normal business activities, larger than usual transaction volume, and transactions with high-risk countries.

5. From time to time, JPM employees did reach out to EMTC or Essilor to communicate about transactions that were potentially suspicious. These communications confirmed Plaintiffs' understanding that JPM was conducting the transaction monitoring that JPM described to Plaintiffs. However, when presented with the highly suspicious pattern of fraudulent transactions at issue in this action, JPM inexplicably failed to notify or contact EMTC or Essilor.

6. JPM was aware of a dramatic change in activity in the NY Account beginning in September 2019, but JPM did not sound the alarm. The average monthly dollar volume of transactions skyrocketed from $15 million to over $100 million and JPM never asked for, or received, an explanation for the increased volume. The number of payment orders doubled relative to historic averages. During the three-month period of the fraud, EMTC repeatedly exceeded the DOL, which was expressly agreed to by JPM, and JPM failed to notify or contact EMTC or Essilor.

7. The fraudulent transfers were all made in round dollar amounts (*i.e.*, no cents), which was a dramatic departure from prior periods where round dollar transfers were relatively infrequent. The identity of the typical transfer recipients also changed dramatically. Previously, the typical recipients were established EMTC trading partners, or companies obviously operating in the same optical industry as Essilor and EMTC, with accounts at established international banks. During the period when the fraudulent transfers were made, most of the transfers went to shell companies, or companies that were not involved in the optical industry, with accounts at regional banks, often in high-risk jurisdictions.

8. JPM was aware of other red flags. During the period when the fraud was perpetrated, the timing of second approvals for the transfers at EMTC occurred immediately after the first approval, which was unusual and is a suspiciously short period of time. JPM was also aware that one of the fraudsters provided false reports to the Bank of Thailand, misrepresenting the identity of the beneficiaries of fraudulent transfers.

9. If JPM had reported these red flags to Essilor and EMTC, the fraud would have been detected in its early stages and Plaintiffs' losses could have been prevented.

10. Pursuant to Section 4-A-204 of New York's Uniform Commercial Code ("U.C.C."), a bank is liable for unauthorized transfers unless it can show that (i) it followed an agreed upon, and commercially reasonable, security procedure for authorization of payment orders *and* (ii) that it acted in good faith. JPM cannot satisfy this test here and, thus, it is liable for the fraudulent transfers. In addition, JPM is liable for violations of common law duties, as set forth herein.

PARTIES

11. Essilor is a French simplified joint-stock company with its principal place of business located in Charenton-le-Pont, France. Essilor is one of the three main subsidiaries of EssilorLuxottica SA, the world's leading ophthalmic optics company. Its proprietary eyewear brands include Ray-Ban and many other leading eyewear brands. EssilorLuxottica is listed on the Euronext Paris stock exchange and is included in the Euro Stoxx 50 index. It has large operations in the U.S., including a global research and development center in Dallas, Texas and production facilities in various cities including Charlottesville, Virginia and Salt Lake City, Utah.

12. EMTC is a Thai limited company with its principal place of business in Bangkok, Thailand. EMTC is a wholly owned subsidiary of Essilor and operates a manufacturing plant in Thailand, one of Essilor's 14 global operation plants. EMTC has a U.S. bank account with JPM (*i.e.*, the NY Account), which it accesses to purchase supplies and conduct other transactions in U.S. dollars.

13. JPM is a national banking association with its home office in Columbus, Ohio.

JURISDICTION AND VENUE

14. This Court has jurisdiction pursuant to 28 U.S.C. § 1332(a)(2) because there is complete diversity of citizenship between the parties and the amount in controversy, exclusive of interest and costs, exceeds $75,000.

15. Venue is proper pursuant to 28 U.S.C. § 1391(b). The NY Account is an account with a JPM branch in this District and a substantial part of the events and omissions giving rise to the claims asserted herein occurred in this District. Additionally, venue is proper as the account terms applicable to the NY Account contain a forum selection clause selecting the jurisdiction of the JPM branch (*i.e.,* New York) as the appropriate forum for disputes.

FACTUAL BACKGROUND

I. The Fraudulent Transfers

16. Essilor, EMTC, and JPM have a long-standing banking relationship. EMTC's NY Account was based in a JPM branch located in New York, NY. The NY Account was opened as part of a larger cash management solution, implemented in March 2017, that also involved certain other JPM accounts utilized by Essilor subsidiaries.

17. From mid-September 2019 until mid-December 2019 (the "Fraudulent Period"), international cybercriminals caused EMTC to make approximately 243 fraudulent payments resulting in the transfer of approximately $272,151,000 out of the NY Account. The funds were deposited to a multitude of straw man accounts located throughout the world.

18. The cybercriminals enlisted a then-current employee of EMTC, Chamanun Phetporee ("Phetporee"), to initiate the fraudulent payment orders. When Phetporee initiated the fraudulent payment orders, she acted beyond the scope of her authority. Phetporee has been taken into custody by Thai law enforcement authorities and charged with multiple crimes.

19. Phetporee was not authorized to approve payment orders from the NY Account on her own. Two separate approvals at EMTC were required to process a payment order. While Phetporee was able to provide the first approval, a separate approval from a specifically designated EMTC employee was required. Phetporee misappropriated the credentials of the designated second approver. In any event, Phetporee's authority, and any second approver's authority, was limited to transactions that were permitted under Essilor's and EMTC's policies and procedures, which do not permit fraudulent transfers.

20. Pursuant to NY U.C.C. § 4-A-204, JPM is liable for all unauthorized transfers from the NY Account unless it can demonstrate (i) that it followed an agreed upon, and

commercially reasonable, security procedure for authorization of payment orders *and* (ii) that it acted in good faith. Good faith in this context includes honesty in fact and actions that comport with the parties' reasonable expectations as to how the security procedures would operate.

21. JPM cannot make the required showing because it overlooked numerous highly suspicious facts relating to the payment orders that alerted it, or should have alerted it, to the fraudulent nature of the transactions.

II. Plaintiffs Reasonably Understood that JPM Would Report Suspicious Activity

22. Based on their communications, Plaintiffs reasonably understood that JPM would monitor the NY Account, including for fraud prevention and AML compliance. JPM's website contains a page entitled "Global Financial Crimes Compliance," which emphasizes its commitment to combatting global financial crimes and describes measures JPM purportedly implemented in furtherance of its commitment. This webpage states:

> JPMorgan Chase & Co. ('JPMC') and each of its majority-owned subsidiaries (together with JPMC, the 'Firm') are firmly committed to participating in international efforts to combat money laundering and the funding of terrorist activities. . . . The Firm has implemented a risk-based global Anti-Money Laundering ('AML') Compliance Program ('AML Program') designed to comply with AML laws and regulations in the U.S.

23. The purpose of an AML program is to deter criminals from transferring and obtaining illicit funds through the financial system, and JPM was legally obligated to ensure it did not support money laundering activities. JPM was required to monitor EMTC's account activity, including any unusually large volume of transfers, and report suspicious activity. It was further required to develop an understanding of EMTC's business sufficient to assess whether transactions were suspicious. Suspicious activities include unusual transaction patterns, a larger than usual volume of transactions, and transactions with high-risk countries. JPM was supposed

to provide training to its employees sufficient to ensure they could identify suspicious transactions and adapt to emerging criminal methodologies.

24. Section 17.5 of the Account Terms applicable to the NY Account confirms that JPM would adhere to its AML policy when administering the NY Account and cautions that adherence to such provision will result in "transaction screening" that may cause delays. That section states, in part:

> Both the Bank and the Customer represent that it shall comply with applicable laws and regulations. *The Bank is required to act in accordance with Bank policies, the laws and regulations of various jurisdictions relating to the prevention of money laundering* and the implementation of sanctions, including but not limited to regulations issued by the U.S. Office of Foreign Assets Control. *The Bank is not obligated to execute payment orders or effect any other transaction where* the beneficiary or other payee is a person or entity with whom the Bank is prohibited from doing business by any law or regulation applicable to the Bank, or *in any case where compliance would, in the Bank's opinion, conflict with applicable law or banking practice or its own policies and procedures*. . . . *Transaction screening may result in delays* in the posting of transactions and/or funds availability. In this context, the Bank may require the Customer to make changes to the activity in the Customer's Accounts, including if necessary to cease and desist from using the Accounts for particular types of transactions or for transactions involving particular parties from time to time.

(Emphasis added).

25. Similarly, Section 17.15 of the Account Terms provides, in part: "To fulfill the Bank's 'know your customer' responsibilities, the Bank will request information from the Customer from time to time regarding the Customer's organization, business. [sic] The Bank may also request further information and/or documentation in connection with the provision of the Services."

26. JPM's Cash Management Services "Welcome Guide" offered assurances of JPM's "commitment to the delivery of the highest standard of service and support available" and a "dedicated Client Service Team" that would provide EMTC with "strategic focus, direction and

excellence in client service and support." Likewise, an email from JPM promised "robust" service, and referenced JPM's ability to "leverage [its] strong expertise to help Essilor with setting up the most efficient and optimized solutions."

27. As noted, the NY Account was opened as part of a broader cash management system among multiple Essilor-affiliated companies. In order to ensure that EMTC, and other affiliates, had sufficient funding to operate, JPM permitted overdrafts, subject to a daily limit, and negative balances would ultimately be settled through the daily cash sweeping process. Under this system, if the balance of any affiliate's account was negative, proceeds would be swept down from the parent company at the end of each day. Conversely, any positive balance would be swept up to the parent. Thus, EMTC would begin each day with a zero balance. JPM described the overdraft limit process in an email noting that:

> intraday overdraft ('IDOD') limits will be set up, either to be shared by the participating entities or applied individually to each bank account participating in the cash pool. We will work closely with Essilor to determine the appropriate overdraft (intraday and overnight) limits required to support your daily transactional requirements. The *usage of these lines will also be monitored on an ongoing basis* to ensure that the limits remain adequate to enable the efficient processing of your transactions.

(Emphasis added).

28. Plaintiffs requested in writing that JPM institute a daily overdraft limit (*i.e.*, a "DOL") of US $10 million for the NY Account. JPM agreed to do so. When implemented correctly, a DOL can, among other things, mitigate against unauthorized and/or fraudulent transfers because it ensures that unusual overdraft activity will be brought to the bank's, the account holder's, and any other relevant parties' attention. JPM should have automatically blocked any transfers that exceeded the DOL and contacted Plaintiffs. The DOL constituted a written instruction from EMTC and Essilor to block any daily transfers from the NY Account

exceeding $10 million. This arrangement was mutually beneficial. Without it, JPM would effectively extend EMTC unlimited credit as its account's balance is set at zero at the beginning of each day. The DOL reflects the Plaintiffs' reasonable understanding that JPM was monitoring the amount of the transfers from the NY Account and should have alerted the Plaintiffs to the unusual fact that the DOL was repeatedly being exceeded during the Fraudulent Period, sometimes by more than $20 million, which could have avoided many later unauthorized and fraudulent transfers.

29. The Federal Financial Institutions Examination Council ("FFIEC") issues guidance concerning security procedures applicable to banks and online transfers, including its bulletin titled "Authentication in an Internet Banking Environment" and a 2011 supplemental bulletin. The FFIEC guidance describes commercially reasonable practices for authenticating users and for performing risk assessment. This guidance further requires banks to include in their layered security program "processes designed to detect anomalies and effectively respond to suspicious or anomalous activity related to . . . initiation of electronic transactions involving the transfer of funds to other parties." If JPM had complied with these standards, the fraudsters could not have executed the fraudulent transfers, which should have been identified as "anomalous activity."

30. From time to time, JPM employees did ask for additional details regarding transfers from EMTC's NY Account. For example, in 2019, JPM sent an email to an EMTC employee and another email to Phetporee (copying this other EMTC employee) inquiring about a message for a $500,000 payment to a beneficiary and relaying a request for further details from "our compliance team." Although JPM sought further information regarding this particular transaction, it failed to identify the suspicious trading activity, described herein. JPM's

compliance inquires and account monitoring confirmed Plaintiffs' understanding that JPM was monitoring account activity and would report any red flags to Essilor and EMTC.

31. JPM also demonstrated that it would block transfers on its own initiative, even when those transfers should have been made automatically because they were executed through the SWIFT (Society for Worldwide Interbank Financial Telecommunications) network. On December 11, 2019, Essilor attempted to transfer $19 million from its JPM account to an account it held in another bank using the SWIFT network. This transfer, which was not fraudulent, was blocked presumably because JPM detected unusual account activities. Despite repeated inquiries, JPM has never explained why it blocked this transfer, but failed to block the fraudulent transfers.

III. JPM Ignored Highly Suspicious Account Activity

32. The transactions from the Fraudulent Period were markedly different than those from January 2017 – August 2019 (the "Pre-Fraudulent Period"), both in terms of the number and aggregate value of payment orders per month, as well as the types of transactions.

A. Transaction Volume Spiked During the Fraudulent Period

33. During the Pre-Fraudulent Period, the average total amount of transfers per month was less than $15 million. During the Fraudulent Period, the average monthly dollar volume of transfers spiked dramatically. In October 2019, approximately $33,222,000 was transferred from the NY Account, *i.e.*, double historic averages. Transfers dramatically escalated thereafter with approximately $119,354,000 in November 2019 and approximately $140,117,000 in December 2019.

34. The number of monthly payment orders out of the NY Account also doubled during the Fraudulent Period, relative to the Pre-Fraudulent Period. In 2017, there was an average of 32 payment orders per month out of the NY Account. In 2018, there was an average

of 54 payment orders per month out of the NY Account. Between January and August 2019, there was an average of 56 payment orders per month out of the NY Account. During the three-month Fraudulent Period, there was an average of 102 payment orders out of the NY account, with over 100 payment orders made in each of October, November, and December 2019.

35. As set forth previously, JPM was required to take note of transfer volumes that were much higher than usual and make further inquiries. If it had done so, the fraudulent transfers could have been avoided, or unwound in the early stages of the fraud, and future fraudulent transfers would have been prevented.

B. The Types of Payment Orders During the Fraudulent Period were Suspicious

36. The types of payment orders initiated out of the NY Account during the Fraudulent Period deviated substantially when compared to the account activity in the Pre-Fraudulent Period. For example, during the Pre-Fraudulent Period, most payment orders out of the NY Account were for a very specific amount of money, down to the cents (*e.g.,* $18,203.96 or $34,270.80), with very limited exceptions. During the Fraudulent Period, there was an uptick in round-number (*i.e.*, no cents) payment orders. In fact, all of the fraudulent transfers were round figures. This dramatic departure from prior periods was highly suspicious and, either alone or with other red flags, should have caused JPM to investigate further and to report these red flags to Plaintiffs.

37. The increase in round-number payments also coincided with payment orders to a variety of new beneficiaries. Most of the beneficiaries during the Pre-Fraudulent Period were either recognizable businesses within the optical industry or subsidiaries of Essilor. It is clear from entity names that many of the beneficiaries during the Fraudulent Period did not operate within the optical industry (*e.g.*, Guangzhou Wendy Hair Products, Citgo Oil Trading LLC,

Maskhoa Coffee Roost Limited, Dekwa Furniture Global, Wealthy Creation Asia Private Limited, Charity Njabili). These are not entities that EMTC had transacted with prior to the Fraudulent Period. Further, transactions made during the Pre-Fraudulent Period were almost exclusively transmitted through the same four large international banks, specifically (1) Citibank N.A., (2) JPMorgan Chase Bank, (3) Standard Chartered Bank and (4) HSBC Bank USA, N.A. The transactions made during the Fraudulent Period, by contrast, were mainly transmitted through small, regional banks located in Southeast Asia, including China and other high-risk jurisdictions.

38. JPM should have conducted further research into the entities that were designated to receive these highly suspicious transfers. If it had done some basic research, it would have quickly confirmed that the vast majority of the fraudulent transfers were being made to shell entities, or to straw man accounts created to facilitate the fraud. Of the fraudulent transfers, 174 went to entities (72 entities in total) that were easily identified as shell entities with no purpose except to facilitate fraud. JPM could have made this assessment by performing Google searches and reviewing incorporation documents. JPM had the capacity to perform this research, as bank AML groups routinely employ such resources to detect potential fraud and money laundering.

39. As noted above, JPM was required to develop an understanding of EMTC's business sufficient to identify transactions that would be considered out of the norm for EMTC. JPM knew EMTC was a manufacturing entity that rarely transacted in round figures and generally only transacted with legitimate trading businesses that maintained accounts at large international banks. The transactions during the Fraudulent Period were dominated by noticeable deviations from EMTC's usual practice and should have prompted JPM to investigate and notify Plaintiffs.

C. Overdrafts Spiked During the Fraudulent Period

40. As noted, JPM agreed to institute a DOL of $10 million for the NY Account. During the three-month Fraudulent Period, the DOL was exceeded at least nine times. In contrast, during the Pre-Fraudulent Period, which spanned three years (or 12 times as long as the Fraudulent Period), no transactions exceeded the DOL during that entire period. The high incidence of overdrafts was further strong evidence of unauthorized account activity. Yet JPM did not notify EMTC and Essilor of the overdrafts or stop transfers from the account that exceeded the $10 million DOL. If JPM had promptly notified Plaintiffs of overdrafts during the Fraudulent Period, it would have alerted Plaintiffs to the fraud. It would also have allowed Plaintiffs to promptly address the larger overdrafts, including two dates on which overdrafts exceeded $30 million (*i.e.,* more than $20 million over the $10 million DOL).

D. The Timing of Approvals was Suspicious

41. JPM's stated security protocol required a two-step verification process. First, a "maker" would initiate a payment order. However, that transaction would not be processed until two separate "approvers" approved the payment order. The transaction log for the NY Account shows that, for 91 of the fraudulent transfers, the second approval occurred *less than 60 seconds* after the first approval. This datapoint, which JPM was aware of because it is reflected in the transaction log created by its own systems, was unusual and was an obvious red flag that one person was providing both approvals. During the Pre-Fraudulent Period, and for non-fraudulent transactions generally, the second approval at EMTC did not take place *for ten hours or more*. The substantially quicker approval times should have caused JPM to question the validity of these transactions and contact EMTC and Essilor.

E. JPM Knew that Phetporee Provided False Quarterly Reports To Regulators

42. JPM also knew, or should have known, that Phetporee provided false quarterly reports of payment orders to a regulator, the Bank of Thailand. Plaintiffs and JPM agreed to a procedure whereby EMTC would send JPM monthly reports for validation prior to submission to the Bank of Thailand. On October 21, 2019, Phetporee sent reports to JPM employees (Siriwan Premplumjit and Knokporn Thongkomol) for review prior to sending them to the Bank of Thailand. The monthly report for September 2019 falsely represented that three transfers were from the NY Account to another EMTC account maintained with JPM in Bangkok. JPM knew, or should have known, this representation was false because the transfers were actually made to third parties, not to another EMTC account. This discrepancy should have prompted JPM to inquire further and notify Plaintiffs of the discrepancy.

F. Called Back and Rejected Payment Orders

43. During the Fraudulent Period, there were an increased number of callback requests, which are requests from EMTC for a return of funds. Phetporee recalled more than 40 payment orders during the Fraudulent Period. During the Pre-Fraudulent period only one order was called back. In addition, JPM initially rejected at least 20 transfers due to errors in the payment orders made by Phetporee during the Fraudulent Period. JPM should have recognized these call backs and rejections as red flags and notified Plaintiffs. If it had, Phetporee's participation in the fraud would have been discovered and the bulk of the fraudulent transactions would have been prevented.

FIRST CAUSE OF ACTION
(Article 4-A of the N.Y. Uniform Commercial Code)

44. Plaintiffs incorporate the paragraphs above as if fully set forth herein.

45. Section 4-A-204(1) of the N.Y. Uniform Commercial Code provides in pertinent part:

> If a receiving bank accepts a payment order issued in the name of its customer as sender which is (a) not authorized and not effective as the order of the customer under Section 4-A-202, . . . the bank shall refund any payment of the payment order received from the customer to the extent the bank is not entitled to enforce payment and shall pay interest on the refundable amount calculated from the date the bank received payment to the date of the refund.

46. The fraudulent transfers at issue were not authorized. Phetporee did not have authority to make transfers without approval from a separately designated second approver at EMTC. Even if the second approval had been provided, Phetporee's authority, and the authority of any second approver, was limited to transactions permissible under Plaintiffs' policies and procedures, which did not permit fraudulent payment orders.

47. Phetporee lacked apparent authority to enter into the fraudulent transfers because JPM knew, or should have known, of highly unusual account activity in the NY Account. A commercially reasonable actor, and certainly a sophisticated bank like JPM, would have been alerted to the fact that the transfers were fraudulent and, thus, unauthorized. At a minimum, the suspicious or unusual account activity would have led a commercially reasonable actor to make further inquiries. If those inquiries were made, they would have confirmed that Phetporee lacked actual authority.

48. Because the fraudulent transfers were not authorized, JPM is required to refund the transfers pursuant to Article 4-A of the N.Y. U.C.C. because JPM cannot establish that it (i)

followed commercially reasonable and agreed upon security procedures; and (ii) acted in good faith and in accordance with the reasonable expectations of the parties.

49. As a result, section 4-A-204(1) of the N.Y. U.C.C. requires that JPM refund the payment orders made during the Fraudulent Period (minus any amounts already refunded or recovered), plus interest.

50. To date, JPM has failed to comply with Section 4-A-204(1) by refusing to refund the payment orders made during the Fraudulent Period (minus the amount already refunded or recovered) to Plaintiffs.

51. As a direct and proximate result of JPM's breaches of its duty, Plaintiffs have suffered damages in an amount to be determined at trial.

SECOND CAUSE OF ACTION
(Breach of Contract)

52. Plaintiffs incorporate the paragraphs above as if fully set forth herein.

53. Plaintiffs entered into a valid and binding agreement governing the NY Account and the broader cash management system that was put in place in 2017 involving EMTC and other Essilor subsidiaries.

54. JPM breached its obligations under the contract.

55. Plaintiffs have performed their obligations under the contract.

56. JPM's breaches caused Plaintiffs to suffer damages in an amount to be determined at trial.

THIRD CAUSE OF ACTION
(Negligence)

57. Plaintiffs incorporate the paragraphs above as if fully set forth herein.

58. As customers of JPM, JPM owed Plaintiffs a duty of care, independent of their contractual agreement, to act in a manner consistent with commercially reasonable standards.

59. JPM violated this duty of care.

60. As a direct and proximate result of JPM's negligence, Plaintiffs suffered damages in an amount to be determined at trial.

PRAYER FOR RELIEF

WHEREFORE, Plaintiffs pray for relief and judgment as follows:

A. Judgment against the Defendant on all causes of action and awarding compensatory damages in favor of Plaintiffs in an amount to be determined at trial, plus interest thereon;

B. Awarding Plaintiffs their reasonable costs and expenses incurred in this action, including counsel fees and expert fees; and

C. Such other relief as the Court may deem just and proper.

JURY TRIAL DEMANDED

Plaintiffs hereby demand a trial by jury on all issues triable by jury.

Dated: April 25, 2022

/s/ William A. Maher

William A. Maher
Steven S. Fitzgerald
WOLLMUTH MAHER & DEUTSCH LLP
500 Fifth Avenue
New York, New York 10110
Telephone: (212) 382-3300
wmaher@wmd-law.com
sfitzgerald@wmd-law.com

Attorneys for Plaintiffs