Muddy Waters Capital LLC
info@muddywatersresearch.com
Director of Research: Carson C. Block

These Terms of Use govern current reports published by Muddy Waters Research and supersede any prior Terms of Use for older reports of Muddy Waters Research, which you may download from the Muddy Waters Research's website.

The reports on this website have been prepared by Muddy Waters Capital LLC ("Muddy Waters Capital"). We refer to Muddy Waters Research and Muddy Waters Capital collectively as "Muddy Waters" and individually these entities are referred to as a "Muddy Waters Entity". **You should assume that, as of the publication date of a Muddy Waters report, Muddy Waters Related Persons (possibly along with or through its members, partners, affiliates, employees, and/or consultants), Muddy Waters Related Persons clients and/or investors and/or their clients and/or investors have a short position in one or more of the securities of a Covered Issuer (and/or options, swaps, and other derivatives related to one or more of these securities), and therefore stand to realize significant gains in the event that the prices of either equity or debt securities of a Covered Issuer decline or appreciate.** Muddy Waters Research, Muddy Waters Capital and/or the Muddy Waters Related Persons intend to continue transacting in the securities of Covered Issuers for an indefinite period after an initial report on a Covered Person, and such person may be long, short, or neutral at any time hereafter regardless of their initial position and views as stated in the research report published by Muddy Waters Research or Muddy Waters Capital. Neither Muddy Waters Research nor Muddy Waters Capital will update any report or information on its website to reflect changes in positions that may be held by a Muddy Waters Related Person. Each report specifies the publisher and owner of that report. All reports are for informational purposes only. Under no circumstances should any of these reports or any information herein be construed as investment advice, or as an offer to sell or the solicitation of an offer to buy any securities or other financial instruments.

Muddy Waters Research is an online research publication that produces due diligence-based reports on publicly traded securities, and Muddy Waters Capital LLC is an investment adviser registered with the U.S. Securities and Exchange Commission. The reports are the property of the applicable Muddy Waters Entity that published that report. This website is owned by Muddy Waters Research. The opinions, information and reports set forth herein are solely attributable to the applicable Muddy Waters Entity and are not attributable to any Muddy Waters Related Person (defined below) (other than the applicable Muddy Waters Entity).

By downloading from, or viewing material on this website, you agree to the following Terms of Use. You agree that use of the research on this website is at your own risk. You (or any person you are acting as agent for) agree to hold harmless Muddy Waters Research, Muddy Waters Capital and its affiliates and related parties, including, but not limited to any principals, officers, directors, employees, members, clients, investors, consultants and agents (collectively, the "Muddy Waters Related Persons") for any direct or indirect losses (including trading losses) attributable to any information on this website or in a research report. You further agree to do your own research and due diligence before making any investment decision with respect to securities of the issuers covered herein (each, a "Covered Issuer") or any other financial instruments that reference the Covered Issuer or any securities issued by the Covered Issuer. You represent that you have sufficient investment sophistication to critically assess the information, analysis and opinion on this website. You further agree that you will not communicate the contents of reports and other materials on this site to any other person unless that person has agreed to be bound by these Terms of Use. If you access this website, download or receive the contents of reports or other materials on this website on your own behalf, you agree to and shall be bound by these Terms of Use. If you access this website, download or receive the contents of reports or other materials on this website as an agent for any other person, you are binding your principal to these same Terms of Use.

This is not an offer to sell or a solicitation of an offer to buy any security. Neither Muddy Waters Research nor any Muddy Waters Related Person (including Muddy Waters Capital) are offering, selling or buying any security to or from any person through this website or reports on this website. Muddy Waters Research is affiliated with Muddy Waters Capital. Muddy Waters Capital is an investment adviser with the U.S. Securities and Exchange Commission and is not registered as investment adviser in any other jurisdiction. Muddy Waters Capital does not render investment advice to anyone unless it has an investment adviser-client relationship with that person evidenced in writing. You understand and agree that Muddy Waters Capital does not have any investment advisory relationship with you or does not owe fiduciary duties to you. Giving investment advice requires knowledge of your financial situation, investment objectives, and risk tolerance, and Muddy Waters Capital has no such knowledge about you.

If you are in the United Kingdom, you confirm that you are accessing research and materials as or on behalf of: (a) an investment professional falling within Article 19 of the Financial Services and Markets Act 2000 (Financial Promotion) Order 2005 (the "FPO"); or (b) high net worth entity falling within Article 49 of the FPO (each a "Permitted Recipient"). In relation to the United Kingdom, the research and materials on this website are being issued only to, and are directed only at, persons who are Permitted Recipients and, without prejudice to any other restrictions or warnings set out in these Terms of Use, persons who are not Permitted Recipients must not act or rely on the information contained in any of the research or materials on this website.

The research and reports presented on this website express the opinion of the applicable Muddy Waters Entity only. Reports are based on generally available information, field research, inferences and deductions through the applicable Muddy Waters Entity's due diligence and analytical process. To the best of the applicable Muddy Waters Entity's ability and belief, all information contained herein is accurate and reliable, and has been obtained from public sources that the applicable Muddy Waters Entity believe to be accurate and reliable, and who are not insiders or connected persons of the Covered Issuers or who may otherwise owe a fiduciary duty, duty of confidentiality or any other duty to the Covered Issuer (directly or indirectly). However, such information is presented "as is," without warranty of any kind, whether express or implied. With respect to their respective research reports, Muddy Waters Research and Muddy Waters Capital makes no representation, express or implied, as to the accuracy, timeliness, or completeness of any such information or with regard to the results to be obtained from its use. Further, any report on this site contains a very large measure of analysis and opinion. All expressions of opinion are subject to change without notice, and neither Muddy Waters Research nor Muddy Waters Capital undertakes to update or supplement any reports or any of the information, analysis and opinion contained in them.

In no event shall Muddy Waters Research, Muddy Waters Capital or any Muddy Waters Related Persons be liable for any claims, losses, costs or damages of any kind, including direct, indirect, punitive, exemplary, incidental, special or, consequential damages, arising out of or in any way connected with any information on this website. This limitation of liability applies regardless of any negligence or gross negligence of Muddy Waters Research, Muddy Waters Capital or any Muddy Waters Related Persons. You accept all risks in relying on the information on this website.

You agree that the information on this website is copyrighted, and you therefore agree not to distribute this information (whether the downloaded file, copies / images / reproductions, or the link to these files) in any manner other than by providing the following link: http://www.muddywatersresearch.com/research/. If you have obtained research published by Muddy Waters Research or Muddy Waters Capital in any manner other than by download from that link, you may not read such research without going to that link and agreeing to the Terms of Use. You further agree that any dispute between you and Muddy Waters Research and its affiliates arising from or related to this report and / or the Muddy Waters Research website or viewing the material hereon shall be governed by the laws of the State of California, without regard to any conflict of law provisions. You knowingly and independently agree to submit to the personal and exclusive jurisdiction of the state and federal courts located in San Francisco, California and waive your right to any other jurisdiction or applicable law, given that Muddy Waters Research and its affiliates are based in San Francisco, California. The failure of Muddy Waters Research or Muddy Waters Capital to exercise or enforce any right or provision of these Terms of Use shall not constitute a waiver of this right or provision. You agree that each Muddy Waters Related Person is a third-party beneficiary to these Terms of Use. If any provision of these Terms of Use is found by a court of competent jurisdiction to be invalid, the parties nevertheless agree that the court should endeavor to give effect to the parties' intentions as reflected in the provision and rule that the other provisions of these Terms of Use remain in full force and effect, in particular as to this governing law and jurisdiction provision. You agree that regardless of any statute or law to the contrary, any claim or cause of action arising out of or related to this website or the material on this website must be filed within one (1) year after the occurrence of the alleged harm that gave rise to such claim or cause of action, or such claim or cause of action be forever barred.

Muddy Waters Capital LLC
(Working from Home)
1007 West College Avenue #304
Santa Rosa, CA 95401
USA

May 13, 2021

Mr. Dan Schreiber
Lemonade, Inc.
5 Crosby Street, 3rd Floor
New York, New York 10013

Open Letter to Dan Schreiber of Lemonade, Inc. (NYSE: LMND)

Dear Mr. Schreiber:

Muddy Waters Capital LLC is short Lemonade because it is clear that Lemonade does not give a fuck about securing its customers' sensitive personal information. This is particularly galling, given that in yesterday's call, you stated Lemonade has worked "so hard" to create a "trustworthy" company. Moreover, Lemonade routinely bashes its competitors for being too old to compete in the digital world.

Sensitive Customer Information has been Indexed by Google, Bing, and the Wayback Machine

In the course of using Lemonade's site to do fundamental business research, it was accidentally discovered that Lemonade's site contains an unforgivably negligent security flaw that potentially exposes its customers' personally identifiable information ("PII"). This vulnerability is so gaping that Google, Bing, and the Wayback Machine have *inadvertently* accessed the site *and indexed* customer PII. By clicking on search results from public search engines, we shockingly found ourselves logged in to and able to edit Lemonade customers' accounts without having to provide any user credentials whatsoever! This vulnerability appears to have existed since at least July 2020, yet it is detectable through an industry standard off-the-shelf security testing application that costs $400 per year. Given that Lemonade is "built on a digital substrate", there are no legacy systems, and Lemonade was founded in an age of mass security breaches, how could it leave the front door wide open for attackers? I can only assume it is due to *callous indifference* to security. Or maybe you personally were distracted by selling $48 million of stock just six months after the Lemonade IPO.

Lemonade's failures possibly implicate costly legal and regulatory breaches. We discovered that one of the crawlers had indexed an EU resident's PII. Considering that Lemonade markets its products directly to EU residents, we believe that Lemonade could have violated the EU's GDPR, which could lead to significant liability. We also believe that Lemonade could have violated the California Consumer Privacy Act and New York's regulations related to the cybersecurity requirements of financial services companies (23 NYCRR Part 500), which might also impose significant liability. We are notifying the various regulators of our findings.

This inexplicably obvious vulnerability gives rise to a range of questions about Lemonade, including:

- If the front door is this wide open, then how well secured are Lemonade's back doors, including its API?
- Lemonade's perceived value lies in part in its data collection – how well-secured is this proprietary advantage?
- Where else in its business has Lemonade cut (or blasted through) corners? (Based on the callous indifference to customer security Lemonade has demonstrated, it is certainly not discouraging for short sellers, such as ourselves, to look at the more traditional aspects of the business for significant problems.)

We call upon Lemonade to take its site offline immediately and fix the vulnerability. (We detail our understanding of the vulnerability below.) We further call upon Lemonade to investigate the scope of the security failure and the personal data it might have exposed, and notify any and all potentially impacted customers.

"Coordinated Disclosure"

We expect that in an attempt to deflect from Lemonade's negligence, it will emphasize that Muddy Waters did not follow the practice of coordinated disclosure, which would have involved us secretly informing Lemonade of the vulnerability and providing it with a reasonable timeline to address it.

Coordinated disclosure is an abject failure. One need only look at the constant drumbeat of news about catastrophic breaches, such as those at SolarWinds and the Colonial Pipeline, to see that time and again, the stewards of our information economy are failing to expend the resources to adequately protect the United States from predators. The state of play is that you stewards assume you'll get a chance to sweep your negligence under the rug when informed of it through coordinated disclosure. You're willing to take your chances with respect to security breaches that become known, with the worst case seemingly being that you'll call in a crisis PR firm to help you craft statements telling everybody that "Securing our customers' information is our top priority".

I have tried other means to hold companies accountable for data breaches, yet have been frustrated in doing so. After being informed that my PII might have been compromised in the Equifax breach, I individually sued Equifax and certain executives, wanting to depose them and understand how they could have failed so spectacularly. Unfortunately the court consolidated my action with the class action, and I received no such relief.

After being revolted for years by the indifference to security shown by companies such as Lemonade, I have concluded that the only way to make a difference is for people like you to be held publicly accountable.

Lemonade.com Security Vulnerability: Scope, Impact, and Remediation

We found a Stored Session Fixation Vulnerability in Lemonade's insurance quoting system. We believe that a vulnerability such as this would typically receive a Common Vulnerability Scoring System (CVSS) score of 10, indicating a critical security risk.

We believe that all Lemonade customers from July 2020 to the present are potentially affected. The scope of the potential damage includes all Lemonade API integration partners, as well as all customers who have submitted PII to Lemonade integration partners via the Lemonade API.

The successful exploitation of this vulnerability apparently results in the disclosure of PII and the

complete compromise of the victim's Lemonade account, including the ability for an attacker to edit account details and apply for or change coverage.

It is unknown whether Lemonade data has been obtained by other crawlers (outside of Google, Bing, and Wayback Machine), by malicious parties, or unintentionally by other users. Due to the ease with which a crawler could inadvertently stumble into a Lemonade user's account; how lucrative the data stored there could be for identity thieves; and the relatively sizeable Lemonade user base, we fear there could be numerous harmed parties, but we are unable to provide an estimate of impact size.

Similarly, we are unable to determine whether this vulnerability has breached Lemonade's infrastructure. This vulnerability can easily be leveraged in phishing campaigns to potentially commandeer user accounts or user data, so we view it to be likely that a breach has already occurred. Lemonade users should be notified and should be on alert for potential follow-up phishing or spearphishing attacks.

It is unknown how long it will take to remediate the vulnerability, scrub the Internet of all copies of stored PII that belongs to the victims, and restore user access. Lemonade should shut down its website, APIs, and mobile application until the vulnerability is verified as fixed by a qualified third party, as there are users currently at risk. We recommend that Stripe, Lemonade's credit card processing partner, also consider disengaging from any integrated systems and monitor its own systems for any indicators of fraud or anomalous behaviour.

Description of the Lemonade.com Vulnerability

[redacted]

[redacted]

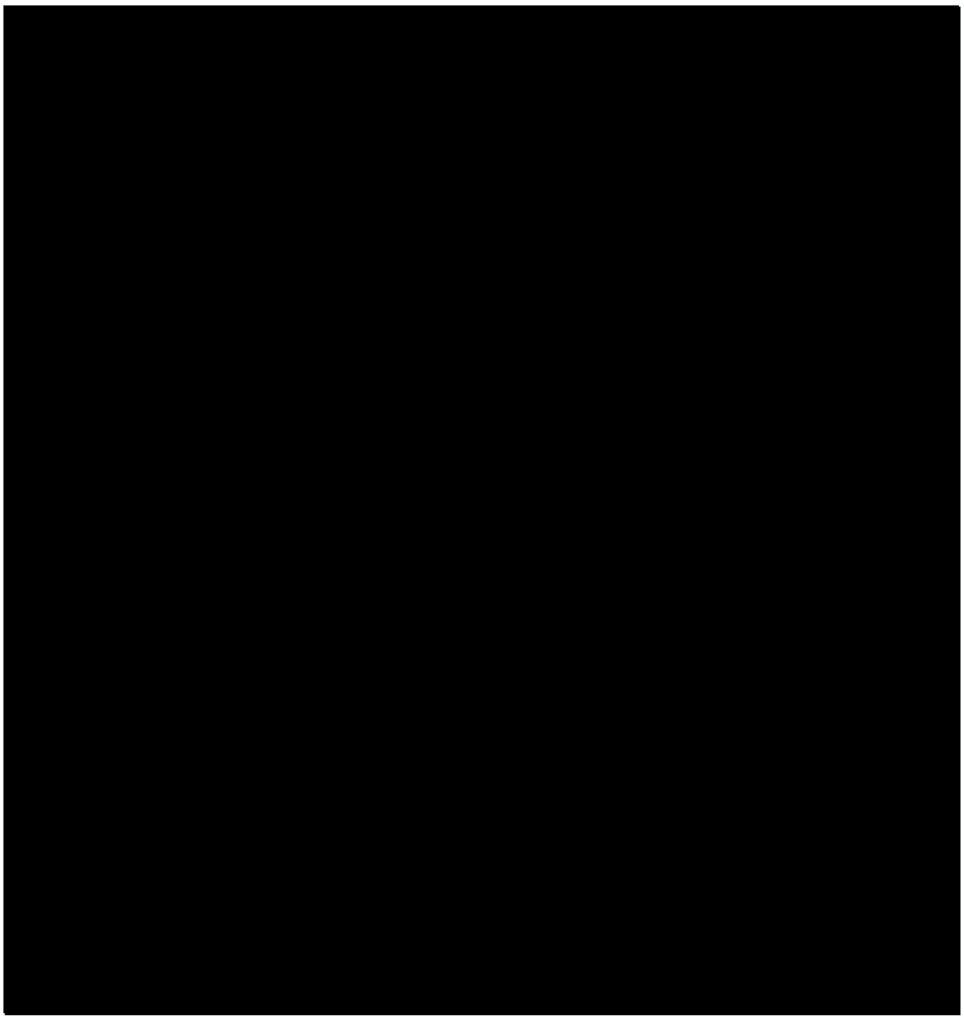
Steps to Reproduce Vulnerability

Reproducing the vulnerability is extremely easy:

[redacted]

Evidence

[redacted]



Conclusion

We note that another activist short seller, The Friendly Bear, has concluded Lemonade's attempt to position itself as an ESG investment is phony and insincere.[1] Based on this egregious failure to secure your customer data, it is hard to believe otherwise. Lemonade has not earned the trust necessary to operate a consumer facing insurance business.

Sincerely,

Carson Block
Muddy Waters Capital LLC

[1] https://friendlybearresearch.com/2020/12/31/how-lemonade-hijacked-the-esg-movement-to-pull-off-the-1-stock-promotion-of-2020/