UNITED STATES DISTRICT COURT
EASTERN DISTRICT OF MICHIGAN
SOUTHERN DIVISION

Jane MH Doe-1 and Jane WP Doe-2,

Plaintiffs,

Case No.:
Hon.
JURY TRIAL DEMANDED

v.

Apple Inc.,

Defendant.

COMPLAINT

1. Defendant Apple Inc. ("Apple") must be held accountable for its continuing failure to adequately protect members of the public from being stalked with its product, the Apple AirTag® ("AirTag").

2. In 2021, Apple released the AirTag knowing full well that it could–and *would*–be purchased and used by abusive, dangerous individuals, to track, coerce, control, and otherwise endanger and abuse innocent victims.

3. And, in 2021, Apple *also* knew that adequate safeguards had not yet been implemented. Nonetheless, the AirTag was made available to the public. Since that time, Apple has played–and continues to play–catch up, quietly introducing new features that fail to curtail the dangers of a product that is now five years old.

4. Apple concedes that *even today* AirTags remain a profound risk to people like Plaintiffs.

5. Apple's acts and practices, as detailed further herein, amount to acts of negligence, product liability, and violations of the Michigan Consumer Protection Act, MCL 445.903, et seq. ("MCPA"), and invasion of privacy law. Plaintiffs seek injunctive and declaratory relief against Apple, correcting Apple's practice of releasing an unreasonably dangerous product into the stream of commerce, misrepresenting the harms associated therewith, and facilitating the unwanted and unconsented to location tracking. Plaintiffs also seek damages.

PARTIES

6. Plaintiff Jane MH Doe-1 is a citizen of the State of Michigan, domiciled in Birmingham. Jane MH Doe-1 is a pseudonym used to protect the privacy of this Plaintiff, whose true identity is known to counsel.

7. Plaintiff Jane WP Doe-2 is a citizen of the State of Michigan, domiciled in Madison Heights. Jane WP Doe-2 is a pseudonym used to protect the privacy of this Plaintiff, whose true identity is known to counsel.

8. Apple is a corporation organized under the laws of the State of California, with its principal place of business in Cupertino, California, and is therefore a citizen of California for purposes of diversity jurisdiction. Apple is an American multinational technology company. Among Apple's flagship items of consumer electronics is the AirTag, and Apple generally oversees all aspects of this

device, including but not limited to its design, manufacture, marketing, and technical support and maintenance.

JURISDICTION AND VENUE

9. This Court has subject matter jurisdiction pursuant to 28 U.S.C. § 1332(a). Each Plaintiff and Defendant are citizens of different States, and the amount in controversy exceeds $75,000, exclusive of interest and costs.

10. This Court has personal jurisdiction over Defendant because:

a. Apple conducts substantial business in the State of Michigan, including selling and distributing AirTags in Michigan, and a substantial part of the events giving rise to the claims occurred in Michigan; and also because

b. Apple has sufficient minimum contacts with the State of Michigan, including pursuant to the Michigan long-arm statute, MCL 600.715, such that the exercise of personal jurisdiction comports with due process. Apple purposefully directed its AirTag product into Michigan, and Plaintiffs' injuries arose out of Apple's forum-related activities.

11. Venue properly lies in this district pursuant to 28 U.S.C. § 1391(b)(2) because a substantial part of the events or omissions giving rise to Plaintiffs' claims, including the stalking and unwanted tracking of Plaintiffs, occurred in this district. Venue also properly lies in this district pursuant to 28 U.S.C. § 1391(b)(1) because Defendant Apple Inc. is a corporation subject to personal jurisdiction in this district with respect to this action and therefore resides in this district under 28 U.S.C. §

1391(c)(2), including through its distribution and sale of AirTags to consumers throughout the State of Michigan.

GENERAL ALLEGATIONS

12. In response to an April 2, 2024, report aired in the United Kingdom on ITV News[1] Apple made the following statement: "We have identified even more ways we can update Airtag safety warnings and help guard against further unwanted tracking." (See Fig. 1)

(Fig. 1)

13. This promise of future, unspecified action comes far too late. Indeed, it is meaningless for Plaintiffs, who already have been harmed in life-altering ways by Apple's recklessness. The time for ensuring adequate safety warnings and better ways to guard against unwanted tracking was years ago, in April 2021, prior to the

[1]ITV News, AirTags becoming "weapon of choice of stalkers" as GPS tracker cases rocket by 317%, YOUTUBE (Apr. 2, 2024), https://www.youtube.com/watch?v=TBhYdgt1FhE.

release of the AirTag. It is unconscionable for Apple to allow a product to remain on the market that is *still* known to be unsafe.

14. Indeed, Apple has always known that any safeguards it purported to build into AirTags would only, in Apple's own words, "deter as opposed to prevent malicious use."

15. Each year, an estimated 13.5 million people are victims of stalking in the United States, with nearly one in three women and one in six men experiencing stalking at some point in their lifetimes.[2]

16. Apple's AirTags have become a critical–and shameful–part of this ecosystem. From 2021 to present, Apple allegedly received over 40,000 stalking reports, at times averaging 1,000 complaints per month.

17. Stalking can manifest in a host of ways, most often through unwanted and repeated behaviors such as phone calls, texts, visits, gifts, internet posts, or any other series of acts that would cause fear in a reasonable person. Regardless of the acts the stalker employs, the common theme of stalking behavior is the fear elicited in the victim.

[2]Stalking Fact Sheet, STALKING PREVENTION, AWARENESS, AND RESOURCE CENTER 1 (SPARC) (2019), https://www.stalkingawareness.org/wp-content/uploads/2019/01/SPARC_StalkngFactSheet_2018_FINAL.pdf.

18. This fear undermines and erodes a victim's autonomy and drastically disrupts day-to-day life. One in eight employed stalking victims miss time from work because of victimization and more than half lose more than five days of work.[3] One in seven stalking victims move as a result of their victimization.[4]

19. Stalking victims suffer much higher rates of depression, anxiety, insomnia, and social dysfunction than the general population. Most victims report a fear of not knowing what will happen in the imminent future. Stalking is one of the significant risk factors for homicide in abusive relationships.

20. No one disputes any of this. Stalking is a serious, well-known, well-documented phenomenon that not only ruins lives, but ends them.

21. Knowing all this, Apple released a small, concealable device that allows any person in the world with an iPhone to continuously and precisely track any other person's location at the low cost of $29.00.

22. Before releasing the AirTag in April 2021, Apple knew that the AirTag would be used as a stalking tool. Apple even designed certain features to mitigate the risk of stalking. But Apple released the product knowing that these features were inadequate to prevent stalking.

---

[3]Katrina Baum, Ph.D., et al., Stalking Victimization in the United States, U.S. DEP'T OF JUST.: BUREAU OF JUST. STATISTICS 1 (January 2009), https://www.justice.gov/archive/ovw/docs/bjs-stalking-rpt.pdf.
[4]*Id.*

23. Specifically, at the time of release, Apple knew that the AirTag's anti-stalking measures were inadequate for at least the following reasons:

a. The notification system for iPhones only alerted users to an unknown AirTag after three days—an eternity in a stalking situation;

b. Android users received no notifications whatsoever, meaning roughly half of the smartphone-using population was completely unprotected;

c. The AirTag's speaker—meant to emit a sound to alert a victim to an unknown AirTag's presence—was easily defeatable, with videos and instructions for disabling it widely available online;

d. The AirTag's form factor—small, lightweight, and easily concealable—made it trivially easy to hide in a victim's belongings or vehicle without his or her knowledge.

24. Apple made a calculated business decision to release the AirTag despite knowing it was inadequately protected against misuse. Apple prioritized market timing and profits over human safety.

25. The consequences of Apple's decision were swift and predictable. Almost immediately after the AirTag's release in April 2021, reports began flooding in from individuals who had been stalked, tracked, and terrorized through the misuse of AirTags.

26. AirTags have been used by stalkers to track victims to their homes, workplaces, and places of refuge. They have been placed in wheel wells of cars, in purses, in jacket pockets, and in children's backpacks.

27. AirTags have facilitated stalking in domestic violence situations, enabling abusers to locate victims who have fled for their safety. In many cases, the victims had no idea they were being tracked until it was too late.

28. The consequences have been as severe as possible: multiple murders have occurred in which the murderer used an AirTag to track the victim. Similarly, individuals have been murdered—or murdered others—when using AirTags to track down stolen property and confront the thieves.

29. Its "stalker proof" protections exposed as totally inadequate, Apple has spent the last five years scrambling to address its failures in protecting people from unwanted, dangerous tracking. To date, most, if not all, of these failures persist, and Apple continues to find itself in the position of *reacting* to the harm its product has unleashed, as opposed to prophylactically preventing those harms. As one commentator observed: "You wouldn't allow a car to come to mass-market without having vigorous testing, so why are we allowing smart tech to just be released and then fixing safety features later?"[5]

[5]Ellie Fry, Inside chilling rise of AirTag stalking as Apple device is branded 'gift to abusers', THE MIRROR (Apr. 24, 2023), https://www.mirror.co.uk/tech/inside-chilling-rise-airtag-stalking-29746435.

FACTUAL ALLEGATIONS

30. The AirTag was introduced in April 2021 as a standalone product. Roughly the size of a US quarter, it is a tracking beacon, marketed to help consumers locate other objects, such as keys or purses.[6]

31. The AirTag uses Bluetooth Low Energy ("BLE") technology to communicate its location. It works by broadcasting a rotating identifier that is detected by nearby Apple devices, which then relay the AirTag's location to Apple's servers through the "Find My" network.[7]

32. BLE signals can be detected at ranges up to approximately 100 meters (approximately 330 feet) in open spaces, though the effective range in real-world conditions is often 30-50 meters.

[6]Apple introduces AirTag, APPLE PRESS RELEASE (April 20, 2021), https://www.apple.com/newsroom/2021/04/apple-introduces-airtag/.
[7]Ryan Mac & Kashmir Hill, Are Apple AirTags Being Used to Track People and Steal Cars?, NEW YORK TIMES (Dec. 30, 2021), https://www.nytimes.com/2021/12/30/technology/apple-airtags-tracking-stalking.html.

Fig. 4

33. The Find My network leverages the billions of Apple devices worldwide to function as a mesh tracking network. Any iPhone, iPad, or Mac that is powered on and connected to the internet can serve as a relay point for an AirTag's location. There are over two billion active Apple devices globally.

34. This means that an AirTag's location can be updated virtually anywhere in the world where Apple devices are present, which is to say, virtually everywhere. The network operates silently, without the knowledge or consent of the Apple device owners who serve as intermediary relay points.

35. Prior to the AirTag's release, numerous commentators, journalists, and advocates warned that small, inexpensive Bluetooth trackers would inevitably be used as stalking tools.

36. In the months leading up to the AirTag's release, technology journalists and domestic violence advocates publicly raised concerns about the potential for location trackers to be weaponized by abusers.

37. Apple was well aware of these concerns. Internal Apple communications confirm that the company anticipated use of the AirTag for purposes of unwanted tracking.

38. Apple's own marketing materials acknowledged that fact. Apple described the AirTag's anti-stalking features as designed to "deter as opposed to

prevent" malicious use—a candid admission that the product was knowingly released with inadequate safeguards.

39. Despite knowing the risks, Apple chose to release the AirTag with only minimal safeguards, including: (a) an audible alert that would sound after three days of separation from its owner's iPhone; and (b) a notification system that would alert iPhone users—but not Android users—to the presence of an unknown AirTag traveling with them.

40. These measures were woefully inadequate. Three days without an alert gives a stalker more than enough time to track a victim's patterns, home address, workplace, and daily routine.

41. Moreover, approximately half of all smartphone users in the United States use Android devices. At launch, these users had absolutely no way to detect an AirTag being used to track them.

42. Even after Apple eventually released a "Tracker Detect" app for Android in December 2021—eight months after the AirTag's release—the app required users to manually initiate a scan and could only detect AirTags that had been separated from their owner for more than 15 minutes.

43. The Tracker Detect app was widely criticized as ineffective. Unlike the automatic notifications provided to iPhone users, the app required affirmative action

by the Android user, who would have no reason to suspect he or she was being tracked in the first place.

44. Shortly after the AirTag's release, reports of AirTag-facilitated stalking began appearing in news media across the country and around the world.

45. In January 2022, multiple police departments issued public warnings about AirTags being used to track individuals without their consent, particularly being placed on vehicles.

46. Despite these reports, Apple did not recall the AirTag. Instead, Apple issued a statement acknowledging that a "small number" of AirTags had been "misused" and promising future updates to address the issue.

47. In February 2022, Apple announced that it would reduce the time before an unknown AirTag would emit a sound from three days to a random interval between 8 and 24 hours. Even this reduced interval provides a stalker with ample time to determine a victim's home address, workplace, and routine.

48. Apple's incremental, piecemeal approach to safety—implementing half-measures only after public outcry—demonstrates that Apple has consistently prioritized product sales over consumer safety.

49. Throughout 2022 and 2023, reports of AirTag stalking continued to mount. Law enforcement agencies across the country documented hundreds of cases involving AirTag-facilitated tracking.

50. In many of these cases, victims reported that Apple's anti-stalking measures failed to alert them in a timely manner or failed altogether. Some victims only discovered AirTags after finding them during physical inspections of their vehicles or belongings.

51. The audible alert feature proved particularly ineffective. The AirTag's speaker is small and produces a sound that is easily drowned out by ambient noise, particularly when the AirTag is hidden in a vehicle's wheel well or undercarriage.

52. Moreover, instructions for disabling the AirTag's speaker are widely available online. Stalkers can trivially silence the device by removing or damaging the speaker, rendering Apple's primary physical alert mechanism useless.

53. The notification system for iPhone users has also proven unreliable. Users report receiving alerts inconsistently, sometimes not receiving them at all, or receiving them only after extended periods of being tracked.

54. Apple has been aware of these systemic failures since at least mid-2021 yet has failed to implement adequate solutions.

55. All of the above instances—while harrowing—do not come close to exposing the true scope of AirTag stalking. As noted above, from April 20th, 2021 to April 5th, 2024, Apple received over 40,000 stalking reports, over 1,000 complaints per month on average.

56. Despite this staggering volume of reports, Apple has failed to implement safeguards adequate to protect consumers from unwanted tracking. Apple's piecemeal approach to safety updates has consistently lagged behind the documented harms.

57. Apple has the technological capability to implement more robust anti-stalking measures but has chosen not to do so, prioritizing the AirTag's tracking functionality and user experience for legitimate users over the safety of stalking victims.

58. Even for users of Apple's own iPhone operating system, iOS, the protection against unwanted AirTag tracking remains grossly inadequate.

59. The "Item Safety Alerts" feature on iOS is designed to notify users when an unknown AirTag appears to be traveling with them. However, the system relies on algorithmic determinations that frequently fail to detect tracking in a timely manner.

60. The notification system requires the unknown AirTag to be separated from its registered owner and travel with the victim for a period of time before any alert is triggered. During this window, the stalker can freely monitor the victim's movements.

61. The alerts are easily missed. They appear as standard push notifications that can be buried among dozens of other notifications, swiped away accidentally, or simply not noticed.

62. In the modern era, the "alert" is not adequate notice of an unwanted device of an unwanted device being used to track and stalk a victim.

63. Even when a user receives an alert and identifies an unwanted AirTag, the remediation options are limited. The user can play a sound to try to locate the AirTag and can disable it by removing the battery. However, the stalker can simply deploy another AirTag.

64. Apple does not provide iOS users with real-time scanning capabilities that would allow them to immediately detect all nearby AirTags. Users must wait for Apple's system to determine, on its own timeline, that an AirTag may be tracking them.

Inadequate Remedies for Android Users

65. The protections available to Android users are even more deficient than those available to iOS users. For the first eight months following the AirTag's release, Android users had absolutely no means of detecting an AirTag tracking them.

66. In December 2021, Apple released the "Tracker Detect" app for Android devices. The app was widely criticized as inadequate because it required

manual scanning—users had to affirmatively open the app and initiate a scan to detect nearby AirTags.

67. Unlike the automatic background detection available to iPhone users, Android users had to suspect they were being tracked in order to think to scan for trackers—a Catch-22 that rendered the app useless for most victims.

68. The Tracker Detect app could only identify AirTags that had been separated from their owner for at least 15 minutes, and even then, detection was unreliable due to the intermittent nature of Bluetooth signals.

69. In May 2023, Apple and Google jointly announced a cross-platform specification for unwanted tracking detection. However, this specification was not fully implemented until 2024, leaving Android users vulnerable for over three years after the AirTag's release.

70. Even with the eventual implementation of cross-platform detection, Android users still receive less timely and less detailed alerts compared to iPhone users, predictably resulting in a two-tiered system in which the protection a person receives depends on which phone they happen to own.

71. Android users cannot leverage the full capabilities of the Find My network to locate an unwanted AirTag with precision. The "Precision Finding" feature, which uses Ultra-Wideband technology to guide a user directly to an AirTag, is available only on newer iPhones.

72. Android users cannot view the serial number of a detected AirTag through a device in the same manner as iOS users, limiting the ability to provide law enforcement with identifying information.

73. The disparity in protection between iOS and Android users is not a mere inconvenience—it is a design choice that systematically places approximately half the population at greater risk of being stalked.

74. Apple made this choice knowing that its product would be used to track both iPhone and Android users indiscriminately but chose to provide some (though still inadequate) protection only to users of its own ecosystem.

75. This disparity cannot be justified on technical grounds. Apple possesses the engineering resources and technical capability to provide equivalent protection to Android users but has chosen not to do so.

76. Apple's failure to provide more severely inadequate protection for Android users is particularly egregious given that stalkers specifically target Android users because they know those users are less likely to detect an AirTag.

77. Reports from law enforcement and domestic violence advocates confirm that stalkers are aware of the disparity in detection capabilities between iOS and Android and exploit this knowledge.

78. Apple's own data confirms that a disproportionate number of AirTag stalking victims are Android users, yet Apple has consistently failed to prioritize parity in safety features across platforms.

79. The following chart summarizes the key safety feature deficiencies across operating systems as they existed during the period relevant to Plaintiffs' claims:

Safety Feature	**Operating System**	**Deficiency**
Unknown AirTag Screen Alerts	iOS	**Alert is not immediate**. Originally, the alert would not be triggered until 72 hours. Presently, the time has been shortened to between 4 and 8 hours, but this is still too dangerous a wait time. **Can be disabled inadvertently**. iPhone owners who disable "Location Services" in their phone settings (which is often done for separate, privacy-related reasons) will also be unable to receive Unknown AirTag Alerts, but this consequence is not explained to users. The "alert" cannot be triggered independently. A common problem is that Apple's alert cannot be triggered by the tracked individual. Instead, it pops up at random. Thus, the tracked individual often cannot rely on Apple's "alerts." Or at least, she only may do so if the alert randomly pops up again, in the presence of the person from whom the tracked individual is seeking help (law enforcement; mechanic; friend; etc.).Reliability. The iOS AirTag detection software has

		reported problems regarding (1) consistency and (2) accuracy.
Sound Alerts	iOS and Android	**Alert is not immediate. It cannot be triggered independently**. **Volume is insufficient**. The AirTag alert volume is, at maximum, 60 decibels. This is not loud enough to ensure more likely than not that an individual is actually notified, particularly if the AirTag is muffled due to being placed on the outside of an individual's car, within a purse, wrapped in a noise-cancelling fabric, etc. **Sound is not distinct.** The AirTag chime is indistinguishable from the myriad other sound alerts that people's phones, computers, smartwatches, and the like emit on a constant basis. In the modern era, nothing about the AirTag chime alerts individuals to the significance of its purpose and context. Many individuals are also not aware of the significance of the AirTag sound alert upon hearing it. **Duration**. The AirTag beep is not continuous and will stop before a targeted person can locate the AirTag. **Can be disabled with ease**. As noted above, the AirTag remains functional even when the speaker has been disabled, which fact has become known by many would-be abusers, who have posted online tutorials on how to disable AirTag speakers for more effective stalking.
Disabling AirTags	iOS and Android	**Physical possession of the AirTag is required**. If an individual wishes to disable an AirTag that is being used to stalk her,

		she must do so manually. This means that she needs to (1) find the AirTag, and (2) pop off the cover to remove the battery.[8] However, finding the AirTag is not always possible; or often requires significant cost – for example, mechanics often tell victims that their whole car would have to be stripped to look for the AirTag (a considerable cost). Further, physically dismantling the AirTag necessarily compromises evidence needed in law enforcement action.
AirTag Identifier Reset	iOS (and potentially Android)Android	**Resetting identifiers also resets Apple's unknown tracker search logic.** Publicly available reporting,[9] indicates that an AirTag's identifier(s) automatically change at regular intervals, in order to be privacy protective of the owners. The problem, however, is that when those identifiers re-set, it appears to thwart Apple's "tracking alert logic." [10] If an individual wishes to disable an AirTag that is being used to stalk her, she must do so manually. This means that she needs to (1) find the AirTag, and (2) pop off the cover to remove the

[8] https://support.apple.com/en-us/HT2122

[9] https://www.macworld.com/article/345863/how-to-find-block-disable-airtag-moving-withyou.html ("Another reason why you may not be able to find the AirTag is that it may have changed its identifier (which happens regularly). The Bluetooth ID produced by an AirTag, and by all Apple devices that participate in Find My crowdsourcing, changes on a regular basis to avoid becoming a reverse tracking item: if it were persistent, then someone could track your devices based on the "anonymous" Bluetooth ID. That means that your iPhone or iPad has to notice an AirTag moving with it over a relatively short period of time."

[10] *Id.*

		battery.[11] However, finding the AirTag is not always possible; or else it might require significant cost – for example, multiple people have been told by mechanics that their whole car would have to be stripped to look for the AirTag (a considerable cost). Further, physically dismantling the AirTag necessarily compromises evidence that would later be needed in any law enforcement action.
AirTag Firmware Updates AirTag Identifier Reset	iOS (and potentially Android)iOS (and potentially Android)	**Relies on AirTag owners (i.e., stalkers) to implement.** Many of Apple''s attempts to retroactively improve AirTag safety occur via updates of AirTag firmware. For example, firmware update 2.0.24 enabled a feature wherein iPhone owners who are being tracked could use a precision finding feature to locate an unwanted AirTag.[12] But such firmware updates do not happen automatically, or "over the air." Instead, they require the AirTag owners to implement the updates. In the stalking context, this means that these safety updates must be implemented by the very people who the updates are meant to thwart. **Resetting identifiers also resets Apple's unknown tracker search logic.** Publicly available reporting,[13] indicates that an AirTag's

[11] https://support.apple.com/en-us/HT2122
[12] https://support.apple.com/en-us/102183
[13] https://www.macworld.com/article/345863/how-to-find-block-disable-airtag-moving-withyou.html ("Another reason why you may not be able to find the AirTag is that it may have changed its identifier (which happens regularly). The Bluetooth ID produced by an AirTag, and by all Apple devices that participate in

		identifier(s) automatically change at regular intervals, in order to be privacy protective of the owners. The problem, however, is that when those identifiers re-set, it appears to thwart Apple's "tracking alert logic." [14]
Tracker Detect App AirTag Firmware Updates	AndroidiOS (and potentially Android)	**Low Awareness**. The Tracker Detect App is not bundled into Android operating systems or suite of apps that come with non-Apple manufacturers. In order to use this safety measure, individuals would have to know about it, in the first place, and then seek it out and download it. **Does not run in the background.** Unlike Apple's iOS-specific alerts, Tracker Detect is not "always on," meaning that the user must independently trigger the scan. Thus, the app is only as effective as the user's intuition. **Triggering sound alerts.** The Tracker Detect user must wait 10 minutes before having a "detected" AirTag emit a sound.[15] This is particularly important, as Tracker Detect does not allow for precision finding (i.e., the app does not guide the user towards the AirTag''s location). Thus, the only way for a user of Tracker Detect to locate the AirTag is through triggering the sound. **Relies on AirTag owners (i.e., stalkers) to implement.** Many of Apple's attempts

Find My crowdsourcing, changes on a regular basis to avoid becoming a reverse tracking item: if it were persistent, then someone could track your devices based on the "anonymous" Bluetooth ID. That means that your iPhone or iPad has to notice an AirTag moving with it over a relatively short period of time."

[14] *Id*.

[15] https://thebinaryhick.blog/2022/01/08/androids-airtags-oof/

		to retroactively improve AirTag safety occur via updates of AirTag firmware. For example, firmware update 2.0.24 enabled a feature wherein iPhone owners who are being tracked could use a precision finding feature to locate an unwanted AirTag.[16] But such firmware updates do not happen automatically, or "over the air." Instead, they require the AirTag owners to implement the updates. In the stalking context, this means that these safety updates must be implemented by the very people who the updates are meant to thwart.
Tracker Detect App	Android	**Low Awareness**. The Tracker Detect App is not bundled into Android operating systems or suite of apps that come with non-Apple manufacturers. In order to use this safety measure, individuals would have to know about it, in the first place, and then seek it out and download it. **Does not run in the background.** Unlike Apple's iOS-specific alerts, Tracker Detect is not "always on," meaning that the user must independently trigger the scan. Thus, the app is only as effective as the user's intuition. **Triggering sound alerts.** The Tracker Detect user must wait 10 minutes before having a "detected" AirTag emit a sound.[17] This is particularly important, as Tracker Detect does not allow for precision finding (i.e., the app does not guide the user towards the AirTag's location).

[16] https://support.apple.com/en-us/102183
[17] https://thebinaryhick.blog/2022/01/08/androids-airtags-oof/

		Thus, the only way for a user of Tracker Detect to locate the AirTag is through triggering the sound.

80. Apple was repeatedly put on notice by advocacy organizations, law enforcement, and the media that its Android protections were inadequate, yet failed to take timely corrective action.

81. The National Network to End Domestic Violence, the National Center for Victims of Crime, and other organizations publicly called on Apple to address the disparity in protections between iOS and Android users.

82. Law enforcement agencies expressed frustration with Apple's failure to provide adequate tools for investigating AirTag stalking cases involving Android victims.

83. Multiple state attorneys general raised concerns about the safety of AirTags and the adequacy of Apple's anti-stalking measures, particularly for Android users.

84. Despite this overwhelming evidence of harm and repeated calls for action, Apple's response was incremental at best—releasing minor updates that failed to address the fundamental inadequacy of its anti-stalking measures.

85. Apple had the ability at all relevant times to provide real-time background scanning for Android users equivalent to what it provided iOS users.

86. Apple had the ability at all relevant times to reduce or eliminate the delay between an AirTag beginning to track a victim and the victim receiving an alert.

87. Apple had the ability at all relevant times to make the AirTag's audible alert louder, more persistent, and harder to disable.

88. Apple had the ability at all relevant times to implement design changes that would make the AirTag safer.

89. At all times relevant to this Complaint, alternative feasible designs existed that would have substantially reduced or eliminated the risk of AirTag-facilitated stalking without impairing the product's legitimate tracking functionality.

90. Apple could have required identity verification or account linking before activating an AirTag, which would easily deter stalking, and is what any prudent design and manufacture of this type should minimally have.

91. Apple could have implemented geofencing features that would automatically disable an AirTag's tracking when it remained in proximity to a non-owner's device for a defined period.

92. Apple could have designed the AirTag with a louder, non-removable speaker that would sound immediately or within minutes—rather than hours or days—when separated from its owner.

93. Apple could have made the AirTag physically larger and more conspicuous, reducing the ease with which it can be covertly placed on a victim's person or property.

94. Apple could have released simultaneous and equivalent detection tools for Android users at the time of the AirTag's launch, rather than leaving half the population unprotected for years.

95. Apple could have implemented a mandatory registration system linking each AirTag to a verified identity, enabling law enforcement to quickly identify stalkers.

96. Apple could have partnered with domestic violence organizations and law enforcement prior to launch to develop robust anti-stalking protocols integrated into the product's design.

97. Apple could have implemented rate-limiting features that would prevent a single user from deploying multiple AirTags in close proximity to a non-owner's device.

98. Apple could have designed the AirTag to require periodic re-authentication by the owner, preventing indefinite passive tracking.

99. Apple could have built in tamper-evident features that would render the AirTag non-functional if the speaker were disabled or removed.

100. Each of these alternative designs was technologically feasible at the time of the AirTag's release in April 2021. Apple chose not to implement them.

101. Apple's failure to adopt any of these readily available alternative designs constitutes a defective product design under Michigan law.

102. Law enforcement agencies across the country have struggled to address the epidemic of AirTag stalking due to a combination of inadequate tools provided by Apple and the difficulty of tracing an AirTag back to its owner.

103. When a victim discovers an AirTag, the only identifying information available is a serial number accessible via NFC tap. Obtaining the identity of the AirTag's registered owner requires a subpoena or search warrant directed to Apple—a process that can take weeks or months or, more often than not, never works.

104. During this delay, the stalker remains free to continue his or her campaign of harassment, often deploying additional AirTags and/or escalating behavior.

105. Many law enforcement agencies lack the technical expertise to properly investigate AirTag stalking cases, and Apple has not provided adequate training or support to assist these agencies.

106. The Federal Trade Commission has taken notice of the dangers posed by products like the AirTag. The FTC has publicly stated that companies have a

responsibility to build safety features into their products before release, not after harm has occurred.

107. In multiple enforcement actions and policy statements, the FTC has emphasized that companies cannot disclaim responsibility for foreseeable misuse of their products, particularly when that misuse was known to the company prior to the product's release.

108. The FTC has specifically identified location tracking devices as products requiring heightened safety measures due to their obvious potential for misuse in stalking and domestic violence contexts.

109. Apple's knowledge of the AirTag's dangers, combined with its failure to implement adequate safeguards, constitutes precisely the type of conduct that the FTC has identified as warranting enforcement action.

110. Multiple state legislatures have enacted or proposed legislation specifically addressing the misuse of Bluetooth tracking devices for stalking, further demonstrating that the risks posed by products like the AirTag are well-known and foreseeable.

111. Apple's failure to adequately address these risks is not merely negligent—it reflects a conscious disregard for the safety of consumers in pursuit of commercial gain.

112. Apple has generated billions of dollars in revenue from AirTag sales and the broader Find My ecosystem while externalizing the costs of its product's victimization onto the victims themselves, law enforcement, and society at large.

113. Apple's AirTag has been priced at $29 per unit, making it one of the cheapest and most accessible stalking tools ever created. Apple has sold tens of millions of AirTags since the product's launch.

114. The low cost and wide availability of AirTags have materially enabled and enhanced stalking, making it accessible to virtually anyone with $29 and an iPhone—regardless of his or her technical sophistication.

115. Prior to the AirTag, effective GPS tracking devices were expensive, required monthly cellular subscriptions, and were relatively large and difficult to conceal. The AirTag eliminated all of these barriers.

116. Apple knew that by dramatically reducing the cost and complexity of location tracking, it was creating a product that would enable stalking because the primary purpose of the produce is to track—the same purpose of those who want to stalk. Yet, Apple, released the product without adequate protection anyway.

117. The harms caused by Apple's AirTag are ongoing. As of the date of this filing, Apple continues to sell AirTags with safeguards that remain inadequate to protect consumers from unwanted tracking, and the stalking by use of the product is widespread.

118. Plaintiffs were direct victims of the deficiencies described above. The AirTag's inadequate anti-stalking measures failed to protect Plaintiffs from being tracked without their knowledge or consent, resulting in severe physical, emotional, and psychological harm as described more fully below.

PLAINTIFFS' EXPERIENCES WITH AIRTAGS

119. Plaintiff Jane MH Doe-1 resides in Birmingham, Michigan. Beginning no later than approximately July 2026 and continuing through the present, Jane MH Doe-1 has been repeatedly stalked and tracked by a former romantic partner using concealed tracking devices, including at least one Apple AirTag.

120. Jane MH Doe-1's stalker repeatedly appeared at her locations uninvited, demonstrating real-time knowledge of her movements. On July 2, 2026, the stalker appeared at a park where Jane MH Doe-1 was present even though her car was hidden behind a truck, confirming he was tracking her electronically rather than visually. On July 3, 2026, the stalker knew Jane MH Doe-1 was at a fireworks event she had not told him about.

121. On July 18, 2026, Jane MH Doe-1 moved her camper out of a campground where she had been a member for ten years because her stalker kept appearing there, but the stalker still located her. On July 23, 2026, the stalker appeared at Jane MH Doe-1's new residence.

122. On July 25, 2026, Jane MH Doe-1's twelve-year-old son found an Apple AirTag concealed in her car. Jane MH Doe-1 and her son disposed of the AirTag by throwing it into Lake Huron.

123. Jane MH Doe-1 uses an iPhone. Jane MH Doe-1 did not receive any notification from Apple that she was being tracked by an unknown AirTag. Apple's notification system—which purports to alert iPhone users to unknown AirTags traveling with them—failed to protect Jane MH Doe-1.

124. As a consequence of the stalking facilitated by Apple's AirTag, Jane MH Doe-1 feared for her life and her child's life. Jane MH Doe-1 was forced to leave a birthday party at a park because her stalker appeared. Jane MH Doe-1 was expelled from a campground she had frequented for ten years because her stalker kept showing up. Jane MH Doe-1 lives in constant fear and feels perpetually unsafe.

125. Jane MH Doe-1 reported the stalking to friends and family members who witnessed the stalker's behavior.

126. Jane MH Doe-1 has suffered significant emotional and psychological harm, including fear for her life and her child's life, loss of autonomy, disruption of her daily activities, and severe emotional distress.

127. Plaintiff Jane WP Doe-2 resides in Madison Heights, Michigan. On or about March 8, 2023, Jane WP Doe-2 moved into a new apartment after leaving an abusive relationship of four years. Jane WP Doe-2 did not disclose her new address

to her former romantic partner. Nevertheless, on the same day she moved in, the stalker appeared at her new apartment, demonstrating real-time knowledge of her location.

128. On the night Jane WP Doe-2 moved in, she observed a man walking slowly around her car. She did not initially recognize him because her car was parked under a port and it was dark. As she was on the phone with her sister describing what she believed to be an attempted car theft, the man began banging on her apartment door. She then recognized the intruder as her former partner, who fled the scene. Upon inspecting her car, Jane WP Doe-2 discovered that it had been keyed.

129. Approximately two weeks later, Jane WP Doe-2 discovered an Apple AirTag concealed under the backseat of her car. The stalker had placed the device there without Jane WP Doe-2's knowledge or consent in order to track her movements and locate her new residence.

130. The stalking and harassment did not cease after discovery of the AirTag. The stalker entered Jane WP Doe-2's apartment building on multiple occasions, wrote messages on her door, and keyed her car multiple additional times.

131. Jane WP Doe-2 was using an Android phone at the time the tracking began. Jane WP Doe-2 did not receive any notification from Apple that she was being tracked. Jane WP Doe-2 did not have Tracker Detect or any similar application installed. It was not until Jane WP Doe-2's niece visited with an iPhone that an

AirTag alert was triggered on the niece's device, revealing the presence of the unknown AirTag. At least two weeks elapsed between when the tracking began and when the AirTag was detected—and likely longer.

132. Jane WP Doe-2 reported the stalking to law enforcement at the Madison Heights Police Department in approximately April 2023. No meaningful action was taken by law enforcement. Jane WP Doe-2 also reported the stalking to her employer and to friends and family.

133. As a consequence of the AirTag-facilitated stalking, Jane WP Doe-2 suffers from severe anxiety, loss of sleep, shock to her nervous system, and constant fear of what her stalker is capable of doing. Jane WP Doe-2 is still living in the same apartment because she cannot afford to move, and she is constantly looking over her shoulder.

134. Jane WP Doe-2 has also suffered property damage from the repeated keying of her car and vandalism to her home.

135. Each Plaintiff was a direct victim of the deficiencies described above. The AirTag's inadequate anti-stalking measures failed to protect each Plaintiff from being tracked without her knowledge or consent, resulting in severe emotional and psychological harm.

COUNT I
(Negligence)

136. Plaintiffs incorporate by reference their prior allegations as if fully repeated.

137. Apple owed Plaintiffs a duty of reasonable care in its design, marketing, and introduction into the market of its AirTags. Under Michigan law, the existence of a duty is determined by examining the foreseeability of the harm, the degree of certainty of injury, the closeness of connection between the conduct and injury, the moral blame attached to the conduct, the policy of preventing future harm, and the burdens and consequences of imposing a duty and the resulting liability for breach. *See Moning v. Alfono*, 400 Mich. 425, 432-34 (1977) (holding that whether "a manufacturer, wholesaler and retailer of a manufactured product owe a legal obligation of due care to a bystander affected by use of the product, and whether defendants in violation of that obligation created an unreasonable risk of harm in marketing slingshots directly to children is for a jury to decide").

138. As detailed in the paragraphs above, Apple's course of action in designing, marketing, and rushing AirTags to market without adequate safety features – without the safety features Apple itself determined were needed to protect people from unwanted tracking, and without the safety features it represented to the public were present for AirTag – caused a foreseeable risk of the injuries Plaintiffs suffered here.

139. Apple's duty of care here is further supported by considerations of public policy that favor protecting individuals from foreseeable, technology-facilitated stalking and abuse, particularly applying the law to the facts of the modern era.

140. Apple's duty of care is further supported by the fact that the harm was extremely likely, if not virtually certain, to occur; because the magnitude of the burden to guard against the foreseeable injury is most feasible with respect to Apple as the party who designed and controls the products and networks enabling AirTags; and because public and legislative policy considerations favor placing the burden on Apple.

141. The legislative policy of the State of Michigan further supports that Apple has a duty to protect individuals from unauthorized electronic surveillance of their persons, movements, and private affairs. Under MCL 750.539*l*, no person shall install or place a tracking device on another person's vehicle without that person's knowledge and consent, subject to certain statutory exceptions not applicable here. Under MCL § 750.411h(1)(f)(vii), stalking is prohibited, by among other things, "[p]lacing an object on, or delivering an object to, property owned, leased, or occupied by that individual."

142. Apple further owed Plaintiffs a duty of care arising from its voluntary undertaking in designing, marketing, and deploying the inadequate safeguards

associated with AirTags. Apple did not merely manufacture a product, but affirmatively undertook to design and deploy a compact, low-cost, location-tracking device equipped with safeguards that it represented to the public as protective against stalking. Thus, Apple voluntarily assumed a duty to perform the undertaking with reasonable care.

143. Apple breached its duty of care by rushing AirTags to market with inadequate safeguards to prevent their use for stalking purposes.

144. This breach of duty by Apple was the cause in fact of Plaintiffs' injuries because, absent Apple's conduct, the AirTag stalking would not have occurred.

145. This breach of duty by Apple was also the proximate and legal cause of Plaintiffs' injuries because Plaintiffs' injuries were the natural, foreseeable, and probable consequence of Apple's conduct in rushing its AirTags to market without adequate safety features.

146. Apple's breach of duty is further apparent because Apple's product caused a tracking device to track the position or movement of Plaintiffs without their consent, in violation of MCL 750.539*l*. Moreover, the stalking conduct here was foreseeable. It was the precise risk Apple's design intended, and against which Apple could have guarded, but knowingly failed to do so.

147. As a direct and proximate result of Apple's negligence, Plaintiffs suffered actual damages, including mental suffering, fear, anxiety, severe emotional distress, and physical harm arising from being tracked and stalked.

148. Plaintiffs further seek exemplary damages in an amount to be determined at trial because Apple's conduct constituted gross negligence, demonstrating an entire want of care which would raise the belief that the act or omission complained of was the result of conscious indifference to the rights, welfare, or safety of the persons affected. Apple had actual knowledge that its product was defective and that there was a substantial likelihood that the defect would cause the type of injury suffered by Plaintiffs, and Apple willfully disregarded that knowledge, sufficient to support an award of exemplary damages under MCL 600.2949a. Exemplary damages are warranted to deter Apple from engaging in future misconduct.

COUNT II
(Product Liability - Design Defect)

149. Plaintiffs incorporate by reference their prior allegations as if fully repeated.

150. Apple designs, manufactures, distributes, and sells its AirTag product.

151. Under Michigan law, a manufacturer or seller is liable for a defective product that causes harm when the product's design renders it not reasonably safe. MCL 600.2946.

152. A product is defectively designed if a reasonably prudent manufacturer would not have placed the product on the market given the product's risks, or if there existed a practical and technically feasible alternative design that would have prevented the harm without significantly impairing the product's utility. *See* MCL 600.2946(2); *see also Moning v. Alfono*, 400 Mich. 425 (1977).

153. Moreover, a manufacturer is not shielded from liability for harm caused by misuse of a product if such misuse was reasonably foreseeable. MCL 600.2947(2).

154. The AirTag's design was defective and unreasonably dangerous because, at the time it left Apple's control, the foreseeable risks associated with its design exceeded any utility associated with that design, and the AirTag failed to perform as safely as an ordinary consumer would expect.

155. The AirTag's susceptibility to use by stalkers was an inevitable condition of the product resulting from its design that made the product defective and unreasonably dangerous at the time the product left Apple's control, and which proximately caused Plaintiffs' injuries.

156. There existed a safer alternative design that, in reasonable probability, would have prevented or significantly reduced the risk of Plaintiffs' injuries without substantially impairing the product's utility. The foreseeable risks associated with the AirTag outweighed any purported benefits:

a. The nature and magnitude of the risks of harm associated with that design in light of the intended and reasonably foreseeable uses, modifications, or alterations of the product was severe in that the AirTag enabled virtually anybody to track someone's precise location in real-time without the victim's knowledge; no one was exempt from this risk, and Apple knew that it was certain to occur.

b. The awareness of product users, whether based on warnings, general knowledge, or otherwise, of risk of harm was low and not at all open and obvious. Apple affirmatively misled the public to believe AirTags were reasonably safe, and that their mobile devices would adequately warn them if they were being tracked.

c. The likelihood that this design would cause harm in light of the intended and reasonably foreseeable uses, modifications, or alterations of the product was very high.

d. The design of the AirTag did not conform to any applicable public or private product standard in effect when the product left the control of its manufacturer, including for example, the recommendations of domestic abuse advocacy organizations.

e. The intended or actual utility of the product, including any performance or safety advantages associated with that design, is low relative to the magnitude and severity of its inherent safety risks.

f. The technical and economic feasibility of using an alternative design was high. Apple designed and developed better safety features but rushed its product to market without those features.

g. The nature and magnitude of any foreseeable risks associated with an alternative design is low, as the enhanced safety features would have served only to provide awareness of unwanted tracking by unsuspecting victims.

157. The AirTag's design defect was the proximate cause of Plaintiffs' injuries because Plaintiffs' injuries were foreseeable as a result of Apple's release of AirTags lacking adequate safety features, and without the release of the AirTag, Plaintiffs' harm would not have occurred.

158. As a direct and proximate result of Apple's defective product, Plaintiffs suffered actual damages, including mental suffering, physical harm, and severe emotional distress, as set forth above.

159. Plaintiffs further seek exemplary damages in an amount to be determined at trial because 'Apple had actual knowledge that its product was defective and that there was a substantial likelihood that the defect would cause the

type of injury that is the basis of this action, and Apple willfully disregarded that knowledge in the manufacture and distribution of the product, sufficient to support an award of exemplary damages under MCL 600.2949a. Exemplary damages are warranted to deter Apple from engaging in future misconduct.

COUNT III
(Violation of the Michigan Consumer Protection Act,MCL 445.903, *et seq*.)

160. Plaintiffs incorporate by reference their prior allegations as if fully repeated.

161. Apple is engaged in "trade" and "commerce" within the meaning of the Michigan Consumer Protection Act, MCL 445.901, et seq. ("MCPA"), through its design, marketing, and sale of AirTags to consumers, including consumers in Michigan.

162. Each Plaintiff is a "person" within the meaning of MCL 445.902(1)(d) who has suffered a loss as a result of a violation of the MCPA.

163. Apple engaged in unfair, unconscionable, and deceptive methods, acts, or practices in the conduct of trade or commerce as defined by MCL 445.903, including but not limited to representing to the public that AirTags included adequate safeguards against stalking and unwanted tracking, while continuing to sell AirTags with knowledge of their propensity for use in stalking. Specifically, Apple represented that AirTags had characteristics, uses, or benefits that they did not have,

and represented that AirTags were of a particular standard, quality, or grade when they were of another, in violation of MCL 445.903(1)(c), (e), and (s).

164. Apple's conduct constitutes unfair, unconscionable, and deceptive methods, acts, and practices within the meaning of MCL 445.903(1), in that Apple's acts and practices offend established public policy, are immoral, unethical, oppressive, and unscrupulous, cause substantial injury to consumers that is not outweighed by any countervailing benefit to consumers or competition, and constitute an injury that consumers could not reasonably have avoided.

165. Apple's acts and practices, as alleged herein, also constitute violations of MCL 750.539*l* (installation of tracking device without consent), which independently serve as a predicate unlawful practice supporting Plaintiffs' MCPA claims.

166. As a direct result of Apple's unfair and deceptive practices, Plaintiffs suffered actual damages, including mental suffering, physical harm, and severe emotional distress arising from being tracked and stalked by means of Apple's AirTag.

167. Plaintiffs have standing to pursue this claim because they are persons who have suffered actual damages proximately caused by Apple's false, misleading, or deceptive acts and practices, or by Apple's unconscionable actions or courses of action.

168. Pursuant to MCL 445.911, Plaintiffs seek actual damages or $250.00, whichever is greater. Plaintiffs further seek an order enjoining Apple from continuing the deceptive practices alleged herein, and an award of reasonable attorneys' fees and costs pursuant to MCL 445.911(2).

COUNT IV
(Invasion of Privacy - Intrusion Upon Seclusion)

169. Plaintiffs incorporate by reference their prior allegations as if fully repeated.

170. Apple intentionally intruded on and into Plaintiffs' solitude, seclusion, and private affairs by designing, deploying, and maintaining a global tracking network that it knew would be—and was—used to geolocate Plaintiffs without their knowledge or consent. Michigan recognizes the tort of intrusion upon seclusion, which requires an intentional intrusion upon the solitude, seclusion, or private affairs of another that would be highly offensive to a reasonable person. *See Doe v. Mills*, 212 Mich. App. 73, 80 (1995).

171. Apple committed an unauthorized and intentional intrusion or prying into Plaintiffs' seclusion by designing, manufacturing, distributing, and operating a product and network infrastructure which it knew could, and foreseeably would, be used to constantly transmit Plaintiffs' precise physical location to any person who purchased and concealed an AirTag on Plaintiffs' person or belongings—and Apple did so without implementing adequate safeguards to prevent such misuse.

172. The matter intruded on Plaintiffs' constant, precise physical location which was private.

173. Plaintiffs had a reasonable expectation of privacy in their constant, precise, physical location. *See* MCL 750.539*l*; *see also* Mich. Comp. Laws § 750.411h (Michigan's anti-stalking statute).

174. This sort of intrusion, transmitting one's constant, precise physical location to known or unknown third parties without one's knowledge or consent, would be highly offensive and objectionable to a reasonable person, and likely to cause mental suffering. This is evidenced by, *inter alia*, Supreme Court precedent, legislation enacted by Congress, and the Michigan Legislature (including MCL 750.539*l*), and countless studies, op-eds, and articles decrying location tracking, particularly in the context of stalking and abuse.

175. As a direct and proximate result of Apple's intrusion, Plaintiffs suffered actual damages, including mental suffering, physical harm, and severe emotional distress, as set forth above. Plaintiffs are entitled to recovery against Apple in an amount to be determined at trial.

176. Plaintiffs further seek exemplary damages in an amount to be determined at trial because Apple's conduct constituted gross negligence, malice, or fraud. Apple had actual knowledge that its product was defective and willfully disregarded that knowledge, sufficient to support an award of exemplary damages

under MCL 600.2949a. Exemplary damages are warranted to deter Apple from engaging in future misconduct.

RELIEF REQUESTED

Plaintiffs request the Court to enter judgment against Defendant, and accordingly, request the following:

a. That judgment be entered against Apple and in favor of Plaintiffs on the causes of action set forth in this Complaint;

b. That judgment be entered against Apple for all injunctive, declaratory, and other equitable relief sought, including but not limited to an order enjoining Apple from further unlawful or unfair practices with respect to the design, manufacture, and release into the market of its AirTags;

c. That Plaintiffs be awarded all damages, including exemplary damages, in an amount to be determined at trial;

d. Reasonable attorneys' fees and litigation costs, pursuant to MCL 445.911(2), and all other costs of suit;

e. All other such other relief as the Court may deem appropriate.

DEMAND FOR JURY TRIAL

Plaintiffs demand a trial by jury of all claims so triable.

Dated: August 10, 2026

Respectfully submitted,

By:/s/*Patrick Lannen*
STINAR LANNEN, PLLC
Patrick Lannen
patrick@stinarlannenlaw.com
Parker Stinar
parker@stinarlannenlaw.com
Erik H. Johnson
erik@stinarlannenlaw.com
Brooke A. Seely
brooke@stinarlannenlaw.com
280 W. Maple Rd., Suite 230
Birmingham, Michigan 48009
(248) 565-2690

Attorney for Plaintiffs Jane MH Doe-1 and Jane WP Doe-2