

December 9, 2025

**SENT BY CERTIFIED MAIL**

Federal Trade Commission, Office of the Secretary  
ATTN: Bureau of Consumer Protection  
Division of Privacy and Identity Protection (DPIP)  
600 Pennsylvania Avenue, NW  
Suite CC-5610 (Annex C)  
Washington, DC 20580

*RE: Request for Investigation: Systematic COPPA Violations by Youth Sports Data Brokers and Leagues (RCX Sports, National Sports ID, App-Order LLC, et al.)*

DPIP,

I represent Douglas Bottoms and Michelle Bottoms (collectively “Bottoms” or “Complainant”) and their son KB aged 12, a flag football player who participates in multiple tournaments around the country. The Bottoms Family live in Fairfax, Virginia. Mr. Bottoms’ work with the Federal government has made him acutely aware of the risk of digital ID for children. KB remains traditionally identified without a digital ID.

This letter is my Clients’ formal request for investigation of Respondents’ COPPA violations.  
**Main point requiring your agency to investigate:**

**Digital ID is not reasonably necessary to verify that a child is 12 years old.  
Respondents are openly violating COPPA, specifically 16 C.F.R. § 312.7,  
which prohibits operators from conditioning participation on the disclosure  
of more personal information than is reasonably necessary.**

Below you will find an Executive Summary (pages 2-3) and my Clients’ official detailed Complaint (pages 4-15) with citations to evidence. I am also enclosing a binder with source documents -- Exhibits A through Z. You can contact me at [greg@gregglaser.com](mailto:greg@gregglaser.com) for electronic copies. Exhibits J-L and V-X are Complainants’ communications with Respondents regarding how Respondents’ COPPA violations injure 12-year old KB and similar children.

My office is available to provide any additional information or assistance you may need to prosecute this important matter for children’s privacy. Please note that I am also working as a lawyer for the national nonprofit organization Children’s Health Defense (CHD), founded by Robert F. Kennedy, Jr.

I will help CHD report to the public periodically on this file at key milestones.

Respectfully submitted,



Greg Glaser

## EXECUTIVE SUMMARY

### I. NATURE OF THE COMPLAINT

This complaint details a widespread industry practice wherein youth sports leagues and data brokers collude to condition a child's participation in sporting events on the mandatory surrender of sensitive Personally Identifiable Information (PII) and biometric data. This "pay-with-data" scheme violates the Children's Online Privacy Protection Act (COPPA), specifically 16 C.F.R. § 312.7, which prohibits operators from conditioning participation on the disclosure of more personal information than is reasonably necessary.

### II. THE RESPONDENTS ("OPERATORS")

The complaint identifies two primary groups of operators acting in concert:

- Group 1 (Exhibits J-L) : RCX Sports (operator of NFL Flag) and National Sports ID (NSID). RCX mandates the use of NSID for age verification.
- Group 2 (Exhibits V-X): Flag Football Life (FFL)<sup>1</sup> and App-Order LLC (doing business as Zorts Sports and Flash Biometrics). FFL mandates the use of Zorts/Flash Biometrics for eligibility.

For clarity, I also distinguish herein between "The Leagues" (RCX, FFL) and "The Data Brokers" (NSID, Zorts).

### III. EVIDENCE OF VIOLATIONS

#### *A. Violation of 16 C.F.R. § 312.7 (Conditioning Participation)*

The Respondents claim that the collection of digital PII, biometric photos, and social media data is required for age verification. However, this requirement is manufactured.

- Proof of Unnecessary Collection: The Complainant successfully obtained "exemption accommodations" from both Respondent groups, allowing for manual, hard-copy age verification (birth certificates and school IDs) without the creation of a permanent digital ID.
- Admission of Capability: In granting these exemptions, the Respondents admitted they can verify age via physical documentation without "unnecessary expense", proving that the digital data collection is not reasonably necessary to participate in the activity. Yet Respondents refuse to offer a COPPA-compliant traditional identification option to the public (i.e., on their websites). So Respondents pattern and practice is to mislead all families by claiming digital ID is required for participation, which is a violation of COPPA.

#### *B. Deceptive Trade Practices & "Hidden" Monetization*

While purporting to collect data solely for "fair play" and eligibility, Respondents utilize the data for unrelated commercial purposes:

- Targeted Profiling: NSID and RCX admit to profiling children's economic situations and interests for marketing and "targeted advertising strategies".
- Revenue Sharing: The Data Brokers provide direct financial incentives ("profit sharing") to the leagues to mandate the use of their digital ID platforms, establishing a coercive financial loop that bypasses parental consent.
- Biometric Aggregation: App-Order LLC utilizes the youth sports mandate to feed a biometric database (Flash Biometrics) intended for broader commercial security applications.

---

<sup>1</sup> Note that United Sports recently assumed operations of FFL. <https://unitedsports.net/united-sports-expands-its-reach-with-flag-football-life-and-beast-of-the-east/>. References herein to FFL are therefore applied to United Sports.

### *C. Unfair Contract Terms & Lack of Control*

Respondents force parents into "contracts of adhesion" where data rights are waived as a condition of play. Privacy policies explicitly state that children's aggregated data is considered a "business asset" transferable during mergers or sales, effectively stripping parents of their right to control or delete the data once collected.

## **IV. SUBSTANTIAL INJURY**

The aggregation of comprehensive digital footprints (including for example biometrics and social media data) on children as young as six creates substantial privacy risks. As noted by the Government Accountability Office (GAO), such aggregated data poses long-term security risks, including potential targeting by foreign adversaries, which constitutes a consumer injury that parents cannot reasonably avoid given the monopoly these leagues hold over youth participation.

## **V. REQUEST FOR RELIEF**

The Complainant requests the FTC compel the Respondents to:

1. **Mandate Voluntary "Opt-In" Defaults:** Require that any digital ID, biometric collection, or commercial tracking profile be offered strictly as a voluntary, opt-in service. The default method for participation must remain a data-minimized, non-digital verification (e.g., physical document review) unless a parent affirmatively elects the digital alternative.
2. **Enforce 16 C.F.R. § 312.7:** Issue a declaratory order that the collection of biometric and social media data is not "reasonably necessary" for the activity of youth sports, thereby prohibiting Respondents from conditioning a child's eligibility on the disclosure of such data.
3. **Prohibit Coerced Third-Party Sharing:** Halt the sharing of children's data with "partners," affiliates, and foreign entities unless parents provide separate, uncoerced consent that is distinct from the consent required to play the sport.

**OFFICIAL COMPLAINT:** Multiple data broker companies and youth sports leagues actively collude together to implement deceptive and unfair practices that result in data profiles of children that are used in ways counter to their original purposes and expectations, causing long-term and substantial harm to children and the country.

**COPPA STATUTE:** 16 C.F.R. § 312.3 (“It shall be unlawful for any operator of a website or online service directed to children, or any operator that has actual knowledge that it is collecting or maintaining personal information from a child, to collect personal information from a child in a manner that violates the regulations prescribed under this part. Generally, under this part, an operator must:... (b) Obtain verifiable parental consent prior to any collection, use, and/or disclosure of personal information from children (§ 312.5); (c) Provide a reasonable means for a parent to review the personal information collected from a child and to refuse to permit its further use or maintenance (§ 312.6); [and] (d) **Not condition a child’s participation in a game, the offering of a prize, or another activity on the child disclosing more personal information than is reasonably necessary to participate in such activity** (§ 312.7)...”

**SUMMARY:** In order to maneuver around COPPA restrictions, multiple children’s sports age verification companies continue to conduct deceptive business practices aimed at coercing and compelling parents to provide their children’s Personally Identifiable Information (PII), to include biometric information, in order to establish digital footprints aggregated to digital IDs that are then deemed as business “assets” to football tournament leagues and their data broker companies. These digital IDs are then monetized through a plethora of ventures to include marketing, adding value to third party or partner companies, or selling them outright as business assets through the sale of the companies themselves. The deceptive practice itself is multifaceted as the companies artificially manufacture the requirement of a youth athlete to obtain their digital IDs, while simultaneously instituting an unconscionable contract of adhesion where the football age verification services condition a child’s ability to play in their associated tournaments based on whether or not their parents attain a digital ID for them. Specifically, implementing a mandatory ‘pay-with-data’ scheme that conditions participation on the waiver of privacy rights is a direct violation of 16 C.F.R. § 312.7. These companies appear to claim they are compliant with COPPA due to the parents signing their children up for these IDs, versus the children obtaining them directly. However, the deceptive practices used to obfuscate the true nature and use of the digital IDs, the aggregated data added to them, and the overall lack of limitations on their broad dissemination to include “third parties,” to include to foreign entities that lack privacy laws designed to protect consumers, results in a situation where many parents simply lack an understanding regarding what they are signing their children up for. Moreover, the companies provide no online alternative allowing parents to opt for traditional ID (i.e., presenting a birth certificate at or before the tournament).

These obfuscations result in what can only be concluded as unfair business practices on many levels;

- 1) First, as described, when signing their children up for a digital ID to simply verify their child’s age for a sports tournament, parents’ expectations are that these digital IDs are being used solely for that intended purpose. Parents don’t understand they are starting a digital profile for their child that will encapsulate nearly every aspect of their child’s digital footprint, to include their social media, texts, etc, that is primarily being collected and leveraged for data brokers’ financial gain.
- 2) Secondly, due to the parents being required to obtain the digital IDs for their children, the children themselves remain likely unaware that the data broker services have been given full permission to collect on nearly every aspect of their digital footprints that will be stored and marketed for unknown, undefined, and presumably indefinite amounts of time. Such aggregation of a child’s data without the child’s full understanding or knowledge, can result

in substantial damage to the child and his or her future. Through the aggregation of their digital footprint nearly every mistake a child makes, every vice, or any hard lesson learned throughout their adolescence, to include puberty, gets recorded as data points for schools, universities, employers, recruiting services, financial institutions, etc, to review in determining potential acceptance, profoundly impacting the child's future. At no time do children expect or comprehend their desire to simply play youth flag football results in this level of invasive surveillance, tracking, or collection of sensitive personal information and its associated potential impact on their futures. Further, there is no mechanism for a child to know what has been collected on them in the digital sphere, nor a mechanism to address complaints or disputes to correct grievances pertaining to their files.

- 3) Thirdly, the data collection services' terms of services and privacy policies create "half-truths," to confuse and obfuscate the collection issue by making it seem as though the data collected will be limited in use and eventually deleted; however, then create loopholes to uncontrolled "third parties" that includes both co-subsiary biometric companies and partnered data broker companies who have no expectations or obligations of deleting data. Additionally, these firms also state that these digital IDs and their associated personal data will be transferred in the case of a merger, sale, bankruptcy, etc of the company, further eliminating parent's or children's control of their personal data. The end result of these loopholes and third party sharing establishes an environment of only perceived control, where no entity has full control or accountability for a child's PII. This lack of control can become amplified with the understanding that no one can fully anticipate future technological advancements, which can result in large-scale hacks of information, or information being used in manners unforeseen by today's users.
- 4) Although companies are allowed to share data with service providers for "internal operations" without parental consent, here these data brokers (NSID/Zorts) reserve the right to use the data for *their own* marketing, third party sales, and profiling, so they lose their status as mere service providers and become third-party data controllers, requiring distinct consent that was never obtained.
- 5) Additionally, the Government Accountability Office (GAO) itself has officially recognized the digital profiles collected, maintained and leveraged financially by commercialized data broker services has resulted in national security risks, as the data in its consolidated form can be used to target military members and their families, blackmailing individuals in order to obtain confidential information, and/or to jeopardize ongoing defense operations. Note that Mr. Bottoms works for the Department of War.
- 6) Finally, it is absolutely imperative to understand the Digital ID requirement these companies impose remains completely manufactured, maintained only through the direct financial incentives, or profit "sharing," between the data brokers and the youth tournament organizations. The perceived separation of the "users" (individual tournaments) and the "Data Brokers" (Digital ID repositories) results in both entities claiming they are compliant with COPPA requirements. However, when paired together these entities are colluding in a mutually beneficial manner that clearly results in coercing and compelling the collection of children's PII in order to participate in sporting activities, while simultaneously not providing an exemption for in-person age eligibility verification. As will be shown by real-life example, when compelled these companies can provide exemption accommodations revolving around less risky age verification alternatives using hard-copy documentation, which successfully eliminate all the previously discussed risks revolving around children's aggregated data and biometric digital IDs.

Additional details regarding these companies and their associated deceptive and unfair business practices are detailed below. We respectfully request the FTC examine the provided information and compel these companies (and issue a formal opinion if necessary to incentivize others within similar industries) to provide exemptions or opt-outs for parents and their children in order to

eliminate substantial injury, while seriously considering advancing the age groups protected under COPPA.

**BACKGROUND:** This complaint focuses on two main groups of companies that when paired together, condition a child's participation in flag football based on providing electronic PII supporting a digital ID. The first group focuses on RCX Sports, who as a flag football tournament organization (a League) uses and requires eligibility data provided by the controller and processor of the data, National Sports ID (NSID) (a Data Broker). The second group focuses on the flag football tournament organization FFL (a League), and the associated digital ID controller, App-Order LLC (a Data Broker). App-Order LLC is comprised of two subordinate companies, Zorts ID and Flash Biometrics (Data Brokers), that work together to provide individual eligibility verification, and in some instances provide individual biometric eligibility verification on-site.

1) **Group 1: NFL Flag, RCX, & NSID:** National Sports ID (NSID) is unequivocally an "operator" under COPPA.<sup>2</sup> It is a commercial online service whose entire business model is to collect, process, and verify the personal information of individuals, a significant portion of whom are children, for the purpose of participating in youth sports. RCX is also an "operator" in this context. RCX cannot simply outsource its data collection to a third party to avoid liability. By mandating the use of NSID and directing parents and children to that specific online platform, RCX becomes party to the collection of that data. And this fact is unrebutted by the terms of use published by RCX (Exhibit A) and NSID (Exhibit T), both of which allow third party sharing. Based on a review of the RCX privacy policy, there is no direct mention of NSID or a partnership between the parties.

**NFL Flag:** NFL Flag is an NFL-licensed property of more than 1,800 locally operated leagues and over 585,000 youth athletes across all 50 states and Canada. (Exhibit B, page 3). Flag football is played by over 20 million people in more than 100 countries, making it one of the fastest growing sports in the world. To gain access to this market, NFL Flag programs are expanding worldwide, already including tournament teams from China, Germany, Australia, New Zealand, Bahamas, Brazil, France, Ghana, Japan, Mexico and the United Kingdom (Exhibit C & Exhibit D). NFL Flag has made it a goal to reaching five million flag football players in China by 2030 (Exhibit E).

“The NFL Flag Championships at the 2024 Pro Bowl Games is a wonderful opportunity to highlight the amazing youth talent that NFL Flag is developing throughout our leagues around the world,” said Izell Reese, CEO of RCX Sports, executive director of NFL Flag and a Global Flag Football Ambassador.” (Exhibit D, page 2)

---

<sup>2</sup> 16 C.F.R. § 312.2 (“Operator means any person who operates a website located on the internet or an online service and who collects or maintains personal information from or about the users of or visitors to such website or online service, or on whose behalf such information is collected or maintained, or offers products or services for sale through that website or online service, where such website or online service is operated for commercial purposes involving commerce among the several States or with one or more foreign nations; in any territory of the United States or in the District of Columbia, or between any such territory and another such territory or any State or foreign nation; or between the District of Columbia and any State, territory, or foreign nation. This definition does not include any nonprofit entity that would otherwise be exempt from coverage under Section 5 of the Federal Trade Commission Act (15 U.S.C. 45).”)

NFL Flag regularly hosts and sponsors flag football tournaments with teams from around the world. According to its 2025-2026 NFL Flag Regional tournament Rules and Guidelines (Exhibit F), NFL Flag requires all participants in its tournaments, to include those under the age of 13, to be age verified through the National Sports ID (NSID) website. Within those guidelines, NFL Flag explicitly states “onsite age verification will not take place under any circumstances. If you do not meet the roster deadline, your child/athlete will not be eligible to participate.” To verify age eligibility, NFL Flag states, “a birth certificate or passport, or state ID may be used. All participants are required to upload school documents, like a report card or progress report, as well as a photo head shot.” Therefore, NFL Flag makes it very clear the company conditions a child’s ability to participate in their games based on requirements to submit children’s PII online, to include photos that can be used for biometrics, to NSID, their affiliated digital ID platform.

**RCX Sports:** RCX Sports is the official operating partner of NFL FLAG, which is the official flag football league of the NFL and the largest youth flag football organization in the U.S.<sup>3</sup> In reading RCX’s Privacy policy (Exhibit A), it becomes clear the goal of collecting children’s data isn’t for age eligibility verification for sports programs, but rather to establish a digital ID that congregates enough information to characterize and profile children for a plethora of marketing objectives. COPPA objections within the RCX privacy policy can be binned into three main categories; profiling, lack of PII control, and security.

**Profiling:** RCX’s privacy policy openly states that they “partner with third-parties to profile a person’s (including children) identified or identifiable economic situation, health, personal preferences, interests, reliability, behavior, location or movements,” (Exhibit A, section 5, last para, page 7) to essentially consolidate both children and adults “digital footprints.” RCX emphasizes “the information they collect automatically may include Personal Information or they may maintain it or associate it with Personal Information they collect in other ways or receive from third parties.” (Exhibit A, section 5, page 5) Additionally, RCX states they may “collect additional information, including Personal Information from third party websites, social media platforms such as but not limited to Facebook, twitter, Instagram, SnapChat, and/or sources providing publicly-available information.” (Exhibit A, Section 4, page 6) RCX warns that they “do not control these third parties’ tracking technologies or how they may be used.” (Exhibit A, section 5, page 7) The RCX policy also states “they may collect sensitive data about individuals and their household,” (Exhibit A, page 3) which can easily include other minors under the age of thirteen, as well as others who in no way consent to collection.

**Lack of PII Control:** RCX’s privacy policy shows a clear lack of control when it comes to handling information pertaining to children. The policy states, they “may disclose aggregated information about our users without restrictions.” (Exhibit A, section 7, page 8) The policy continues to state it can share users’ PII and aggregated information with affiliates, partners, service providers, advertisers, buyers and successors, and “others.” Of additional concern are the details provided under “buyers and successors” that details users’ aggregated data was considered a company “asset” that could be transferred as part of a merger, divestiture, restructuring, reorganization, dissolution, or any other sale or transfer of some or all of RCX’s assets.” (Exhibit A, section 7, page 9) Furthermore, to add ambiguity, the RCX policy states they “may disclose user PII to comply with any court order, law or legal process, including to respond to any government or regulatory request,” (Exhibit A, section 7, page 9) without any restrictions, to include data releases to foreign governments or international governmental organizations.

**Security:** While NFL Flag requires electronic submission of children’s PII, RCX’s privacy policy openly warns “the transmission of information via the internet is not completely

---

<sup>3</sup> [nflflag.com](https://nflflag.com)



secure. Although we have implemented reasonable safeguards and endeavor to protect your Personal Information, we cannot guarantee the security of your Personal Information to our Websites. Any transmission of Personal Information is at your own risk.” (Exhibit A, section 11, page 14) The policy continues that users “should assume that no data transmitted over the internet or stored or maintained by us (RCX) or our third party service providers can be 100% secure,” and therefore RCX “will not guarantee information including Personal Information will not be misused by third parties.” (Exhibit A, section 11, page 15). The security section within RCX’s privacy policy ends by forcing users to agree to terms that eliminates RCX from any liability of misuse, access, acquisition, deletion or disclosure of user’s Personal Information, highlighting not only the lack of security, but an overall lack of accountability on the company’s part to secure children’s PII. Perhaps most troubling is the admission within RCX’s privacy policy that states, RCX “may process, store, and transfer your Personal Information in and to a foreign country, with different privacy laws. In these circumstances, the governments, courts, law enforcement, or regulatory agencies of that country may be able to obtain access to your Personal Information through the laws of the foreign country,” (Exhibit A, section 13, page 15) underscoring the overall lack of focus on securing children’s PII that NFL Flag is requiring be submitted electronically in order for a child to participate in their sporting events.

RCX’s privacy policy states their “website and services are intended for general audiences. They do not knowingly collect, use, or disclose information, including Personal Information from children under the age of 13 or as otherwise defined by local law without prior parental consent. However, to re-emphasize, NFL Flag is conditioning children’s participation in their games and tournaments, to include those under the age of 13, and even under the age of eight, which remains a COPPA violation.

**NSID:** National Sports ID (NSID) is a “Data Broker” that advertises itself as a trusted partner in ensuring fair play and compliance in youth sports, through its streamlined verification process for young athletes. NSID states this verification process revolves around a three stage process; 1) Submitting the necessary documents 2) NSID team members verify the provided documents, and 3) NSID then provides a secure sports ID for the athlete. NSID claims this process “eliminates the need for physical documents,” which isn’t true since they require those very same physical documents to be uploaded to their website for verification (step one above). NSID also claims its electronic process saves time while significantly reducing costs, making it a win-win situation for all involved. (Exhibit G)

However, after closer examination to NSID’s own website, and personal interaction with RCX’s verification process, the “secure sports ID” provided by NSID appears to be more focused on leveraging players’ PII and associated aggregated data, or “digital footprint” to enable “targeted advertising strategies on platforms like Google and Facebook, aiding various sports organizations and businesses in carving their niche online.” (Exhibit H). NSID further states “at NSID, our Sports Digital Marketers understand sports and mesh that with our creative advertising process to run ad campaigns that lead to sales.” To encourage youth sports organizations to require its secure sports ID, NSID emphasizes their “team of NSID Sports Digital Marketing experts can guide you in deploying strategies that will generate more leads from your website. These leads often convert into sales, and potentially into long-term customer relationships. By blending our knowledge of sports and digital marketing, NSID has successfully fostered the growth of numerous youth sports organizations and businesses.” (Exhibit H). Additionally, in an NSID article on its websites titled “Boost Your Youth Sports Product Sales with NSID: *Harness the Power of Target Marketing Within the NSID Verification Process*,” NSID advertises its “laser-focused targeted marketing” approach significantly increases businesses product exposure resulting in 30-40 percent increase in sales. Such emphasis and



detail underscore the NSID verification process, as well as the value of the data collected and aggregated on children and their parents, appears to be the main goal of requiring their digital ID versus age eligibility verification. (Exhibit I). What's even more troubling is the revenue sharing that takes place between NSID and tournament organizations, which NSID refers to as "partnership payments." Here NSID states it will share revenue with tournament organizations if they mandate the use of NSID and/or use NSID's online check-in. Such financial incentives and the coercive nature to make NSID mandatory at tournaments would not be necessary if NSID's secure digital ID was really addressing a hard to fill requirement. However, as will be shown, no such ID is needed, and despite RCX's initial claims, exemptions from NSID's secure Digital ID can be easily accommodated without added risk or expense.

**EXEMPTION ACCOMMODATIONS:** As previously stated, NFL Flag and its operating arm RCX financially incentivizes tournaments to require a digital ID from its associated data broker, NSID. In October 2025, parents of KB requested RCX provide an accommodation to the digital ID requirement. (Exhibit J). RCX responded by cited a portion of the NFL Flag Regional Tournament rules: "in short, NSID is a secure and trusted verification platform used by more than 10,000 athletes each year. Athletes who do not complete the NSID verification process will not be permitted to compete in NFL Flag Regional Tournaments. No Exceptions" (Exhibit J). Parents of KB, a child under the age of 13, then worked with Children's Health Defense (CHD) to highlight the likely COPPA violations that were taking place. A CHD lawyer (Greg Glaser) then notified NFL Flag, RCX, and NSID regarding their COPPA infractions, and requested an opportunity to discuss the issue directly in order to propose methods that would enable NFL Flag, RCX, and NSID to continue performing their age verification functions while simultaneously providing concerned parents better methods to secure and control their children's digital footprints. Part of the conversation specifically requested an exemption accommodation for KB in an upcoming regional NFL Flag sponsored football tournament. In response to CHD, RCX's Chief Operating Officer, Ms. Garland Cooper, reluctantly agreed to KB's exemption accommodation, which required in-person age verification via review of hard-copy birth certificate, U.S. passport, and school ID, while further emphasizing "If you or KB's parents have further questions on NSID's process, we can put you in touch with NSID. But we have no intention on responding to your other questions and claims and will not participate in a phone call or Zoom with you. This one-time accommodation is being offered to avoid unnecessary expense. **We do not intend to offer this option to any other participants.**" This entire email chain is recorded in (EXHIBIT K), and the initial letter to the company, to include the legal analysis concerning the specific COPPA infractions are documented in (EXHIBIT L).

On November 1, 2025, RCX successfully age-verified KB via hard-copy documentation without any hardship or additional expenses. To facilitate the verification process, KB's father accompanied KB during check-in and provided the hard-copy documentation previously requested by RCX. The RCX employee conducting the age verifications removed KB and his father from the line and reviewed the hard-copy documentation away from other viewing parents, ostensibly to limit observation of the exemption process taking place in view of other parents and coaches. Nevertheless, RCX was able to accommodate the exemption in-person, hard-copy, non-digital age verification without additional hardship or expenses, highlighting such a process could be offered and provided to other concerned parents routinely.

**2) Group 2: App-Order LLC (Zorts and Flash Biometrics) & Flag Football Life (FFL):** Zorts is operated by App-Order LLC, a Nevada limited liability company that specializes in providing all-in-one software solutions for communication and data management for sports leagues, city municipalities, state counties, small and medium size businesses, and Fortune 500 companies. The Zorts "Terms of Use and Privacy Policy" (Exhibit M) correctly cites COPPA law by emphasizing the company's inability to legally collect information from children under

thirteen (13) years of age; however, incorrectly concludes that conditioning a child's participation based on mandating baseline requirements for a digital identification remains consistent with federal law. Zorts website advertises ID and age verification to ensure athlete safety and fair play. Per the FFL/Zorts webpage for the "Drip Flag Football Tournament, FFL states "Players must have an active Zorts ID." (Exhibit N) In order to obtain a Zorts ID players must submit their full name and birth date along with a birth certificate, Native Tribal ID or Government Issued ID as verification, as well as a current photo to support the company's facial recognition software powered by Flash Biometrics," another subsidiary to App-Order LLC. Zorts states the provided digitized ID card makes verifying players' eligibility fast, easy and seamless by enabling facial recognition software used during check-ins at tournaments. Zorts claims this modernized approach provides participants a better experience by decreasing the stress normally caused by cumbersome paper and form processes.

Just like RCX and NSID, Zorts/App-Order LLC is unequivocally an "operator" under COPPA.<sup>4</sup> It is a commercial online service whose entire business model is to collect, process, and verify the personal information of individuals, a significant portion of whom are children, for the purpose of participating in youth sports. FFL, Flash Biometrics, App-Order, and any other company using data provided by Zorts is also an "operator" in this context. These companies cannot simply outsource their data collection to a third party to avoid liability. By mandating the use of Zorts ID and directing parents and children to that specific online platform, all the companies using and/or storing that data become party to the collection of that data. And this fact is un rebutted by the terms of use published by Zorts/App-Order LLC, which allows third party sharing. Based on a review of the Zorts' privacy policy, there is no direct mention of FFL or a partnership between the parties.

**App-Order LLC:** App-Order LLC is a private app development company that designs and develops iOS, Android and web applications. App-Order LLC is the parent company of both Zorts Sports and Flash Biometrics. Within the Zorts Sports Terms of Use and Privacy Policy, App-Order and its subsidiary Zorts Sports claims they are not regulated by COPPA since they do not "knowingly collect information from children under 13 years of age." (Exhibit M).

**Zorts Sports:** Zorts serves as as front-end application as well as a Data Broker that aggregates a users' digital footprint. Like RCX and NSID, Zorts' Terms of Service and Privacy Policy enable shortfalls in user profiling, lack of control, and overall security.

**Profiling:** Zorts develops digital profiles through information collected during the process required for age verification such as contact information, location data, unique identifiers, biometric information, photos, proof of identity, age, event information, user preferences, payment information and any other user information provided to the company. Additionally, Zorts requires through its Terms of Service and Privacy Policy for those acquiring a Zorts ID to consent to cookies and third party collection efforts that enable their ability to enhance users' digital footprints with additional publicly available

---

<sup>4</sup> 16 C.F.R. § 312.2 ("Operator means any person who operates a website located on the internet or an online service and who collects or maintains personal information from or about the users of or visitors to such website or online service, or on whose behalf such information is collected or maintained, or offers products or services for sale through that website or online service, where such website or online service is operated for commercial purposes involving commerce among the several States or with one or more foreign nations; in any territory of the United States or in the District of Columbia, or between any such territory and another such territory or any State or foreign nation; or between the District of Columbia and any State, territory, or foreign nation. This definition does not include any nonprofit entity that would otherwise be exempt from coverage under Section 5 of the Federal Trade Commission Act (15 U.S.C. 45).")

information from social media platforms and profiles, or other third party platforms, plug-ins, integrations or applications. Like other data brokers, Zorts states, they “may also use information collected through Zorts Services for research regarding the effectiveness of the Zorts Services and our business planning, marketing, advertising, and sales efforts.” (Exhibit M page 10)

**Lack of Control:** Zorts also states they “may disclose Personal Information to any person performing audit, legal, operational, or other services,” (Exhibit M, page 13) highlighting the loopholes built into their terms of service that eliminates any restrictions on their sharing of aggregated personal information regarding children and/or their parents. Furthermore, much like RCX and NSID, Zorts considers aggregated PII on individuals as an asset that can be sold for profit. Their Terms of Service and Privacy Policy states;

“We may buy, merge, or partner with other companies or businesses and in so doing, acquire or transfer information. We may also assign or otherwise transfer such information in the regular course of business. Information collected through the Zorts Service may be among the transferred business assets. In the event that a portion or substantially all of our assets are transferred to a third party, your information would likely be a transferred business asset, and you hereby agree to such a transfer.” (Exhibit M, page 14)

Zorts admits they “may not be able to control how your Personal Information is treated, transferred or used” in the event of bankruptcy, insolvency, reorganization, receivership or assignment for the benefit of creditors, or the application of laws or equitable principles affecting creditors’ rights. With this, it must be re-emphasized that as a private company App-Order and Zorts are not required to disclose who their investors and creditors are to the SEC or to individual users, which in this case include parents of children being required to obtain a Zorts ID in order to participate in a sporting event.

Zorts claims the company does not have any plans to sell Personal Information; however, admits they share personal information with service providers who provide goods and services or perform other business functions on their behalf. In their Terms of Service and Privacy Policy, Zorts states, “for the purposes of this notice, a “service provider” is not a “third party.” Zorts’ policy clearly states that information is shared with affiliates and partners for marketing and promotional purposes, which implies a commercial benefit to Zorts, whether direct or indirect. Underscoring this is the fact that Zorts’ details in its Privacy Policy, as detailed above, that identity information would be transferred in a merger, partnership, etc as a “business asset.” Furthermore, the children’s biometric data appears to be central to Zorts’ business model, as they “share” extra revenue with partners who support them in their data collection for Zorts IDs. Zorts’ website indicates the company has “shared” \$1.1 Million with event organizers, (Exhibit O) highlighting the financial incentives they provide flag football vendors for enforcing the Zorts ID requirement. The data collected provides the baseline biometric information needed to feed App-Order’s Flash Biometric database, increasing its value as a commercialized security platform for events beyond youth flag football.

**Data Security:** Zorts correctly states they cannot guarantee the security of data being transmitted to its website, therefore, placing any associated risk of such a transfer on the user.

**Flash Biometrics:** Flash Biometrics is a subsidiary of App-Order LLC and a Zorts Sports partner. Zorts CEO states the Flash Biometrics will enable identity verification for large scale

events, governing bodies, and large operators. (Exhibit P) Flash Biometrics website claims their system supports multi-face recognition, enabling fast and accurate verification of an entire group at once, making it ideal for offices, secure zones, educational institutions, or events where large numbers of people need to be verified quickly. Once a face is verified, the system confirms the match in real-time, indicating whether the individual is cleared for access, ensuring only pre-verified individuals gain entry, improving both security and operational efficiency. While Flash Biometrics states its business is built around privacy concerns, no terms of service and/or privacy policy could be found on its website. This raises particular concerns regarding the retention of users' data, to include children. Considering App-Order/Zorts Terms of Service and Privacy Policy, user data will be shared with their partner, in this case Flash Biometrics. Zorts states it will delete unneeded user data; however, **makes no such claim or responsibility for its partners to do so after user data has been shared with them, basically ensuring that once aggregated data is shared it remains retained by its partner, Flash Biometrics.** These points attain broader concern as Flash Biometrics advertises its system will benefit a multitude of entities across the economy including sports and event management, co-working spaces, fitness and health clubs, E-commerce platforms, education and testing centers, financial services, hospitality and travel and private communities and clubs. As such, Zorts Sports' claim that it is collecting user data, to include children's biometrics, to simply support age-eligibility verification for sports is likely just a means to feed data to its larger goal of building Flash Biometrics' database. According to its website and its co-founder, Neil Lenhoff, this database is being developed to verify users' ability to participate in broader aspects of society, to include government, entertainment and international infrastructure, none of which parents are being informed about when submitting for a Zorts ID. (Exhibit Q - Flash Biometrics Website - [flashbiometrics.com](http://flashbiometrics.com), Exhibit R, & Exhibit S)

**Industry Controversy Regarding Biometrics:** As an interesting note, biometric collection within the sports ID verification industry remains a divisive topic. While Zorts Sports highlights its facial recognition as a highlight of its verification process, NSID criticizes the collection and use of biometric information as "permanent and impossible to change if compromised." Discussing the collection of biometric data, NSID further emphasizes;

"Birth certificates can be deleted. Emails can be reset. Passwords can be changed. Faces cannot. That's why biometric data is such a massive liability. If a database storing children's facial scans is ever breached, exposed, or mishandled, those kids can't reset anything. Their face becomes a permanent identifier, circulating where it doesn't belong." (Exhibit U)

In the same article, NSID highlights regarding biometric collection that parents don't realize their child's face is being stored. Parents assume technology used in youth sports is harmless. Most never realize their child's biometric data may be stored for years, accessed by third parties, outlive the vendor, and/or be used for algorithm training without consent. (Exhibit U) While correct, the irony in NSID's admission is that NSID itself requires youth athletes to provide a photo ID. While the provided ID itself may not be saved indefinitely, NSID's own policies state they can aggregate individuals' publicly available data, to include photos, in order to consolidate and create individuals' digital footprints. This demonstrates that even the industry players acknowledge the substantial harm of biometric data collection, further supporting the Bottoms' claim of unfairness.

**ZORTS SPORTS AFFILIATED TOURNAMENT EXEMPTIONS:** Individual tournaments choose whether or not to affiliate with Zorts Sports, which directs the requirement for their

tournament attendees to attain Zorts' digital ID, to include children under the age of 13. To re-emphasize, Zorts Sports financially incentivizes these tournaments through the "sharing" of their profits, as detailed on their website ([Exhibit O](#)). To date, KB's parents have requested and attained exemption accommodations (three of three) from all the Zorts affiliated tournaments they have requested such exemptions from, further underscoring the requirement for children to attain a digital ID is not needed, but rather simply manufactured for financial gains generated by the aggregation, consolidation, and monetization of children's digital footprints. The three tournaments that have granted exemptions from Zorts ID and the affiliated details of these exemptions are listed below;

**AIM HIGH:** (Aim High Summer Classic, July 12, 2025):

KB's parents did not engage in any direct correspondence with Aim High prior to the tournament. To facilitate the verification process, KB's father accompanied KB during check-in and provided the hard-copy documentation previously required by Aim High. Aim High accommodated the in-person exemption using the provided hard-copied, non-digital documents for age verification without additional hardship or expense, highlighting such a process could be offered and provided to other concerned parents routinely.

**AIM HIGH:** (Aim High Turkey Bowl: The Thanksgiving Classic, November 15, 2025)

KB's parents did not engage in any direct correspondence with Aim High prior to the tournament. KB's coach assessed in-person age verification wouldn't be a problem based on the previously provided in-person exemption made at the Summer Classic. To facilitate the verification process, KB's father accompanied KB during check-in and provided the hard-copy documentation previously required by Aim High. Aim High again accommodated the in-person exemption using the provided hard-copied, non-digital documents for age verification without additional hardship or expense, further underscoring such in-person verification processes could easily be offered more broadly to other concerned parents on a routine basis.

**Flag Football Life (FFL):** The Drip Flag Football Tournament, December 7, 2025)

In October 2025, parents of KB requested FFL provide an exemption accommodation to the Zorts digital ID requirement. FFL responded by stating a ZortsID was required for all players to participate, while further emphasizing that;

"FFL does not have an alternative manual verification process. Physical documentation cannot be accepted or substituted for Zorts verification, as it cannot be integrated into our real-time roster and compliance system"

([Exhibit V](#)).

Parents of KB, a child under the age of 13, then worked with Children's Health Defense (CHD) to highlight the likely COPPA violations that were taking place. CHD then notified FFL and Zorts regarding their COPPA infractions, and proposed methods that would enable FFL and Zorts to continue performing their age verification functions while simultaneously providing concerned parents better methods to secure and control their children's digital footprints. This entailed specifically requesting an exemption accommodation for KB in an upcoming FFL sponsored football tournament. ([Exhibit W](#)) In response to CHD, FFL initially indicated they were "working through potential options to make participation an option for KB," however, FFL did not provide any options until again being reminded through an attorney they were in violation of COPPA. At that point, the owner of FFL, Mike Reimel, finally responded with an accommodation for KB, stating "we have come to the conclusion to make an accommodation for your client. Please have them bring a school ID and the Birth Certificate. We will have to verify your client before check in which may take more time than the **facial recognition.**"



(Exhibit X) While this particular tournament hasn't taken place (it is scheduled for December 7, 2025), the exemption accommodation serves as another admission that the digital ID requirement remains a manufactured requirement, that is not needed to perform its intended purpose of age-eligibility verification for youth sports.

**ADDITIONAL CONSIDERATIONS:** Regarding the substantial injury test for unfairness, the *risk* of foreign data leakage constitutes a consumer injury that parents cannot reasonably avoid. In this section, we are not asking the FTC to act as a defense agency, but rather to understand the context that COPPA works in *harmony* with defense objectives.

In October 2025, the Government Accountability Office (GAO) publicly provided the attached report (Exhibit Y) to Congressional Defense and Intelligence Committees regarding the urgent need for the Department of Defense to acknowledge and mitigate the dangers directly associated data brokers and their business models revolving around establishing digital footprints on military members and their families. The report specifically details how such data aggregation can be sold over the dark web and used by foreign adversaries to disrupt DoD missions and endanger military personnel. It must be noted, many of the above detailed companies, most notably RCX and NSID, employs foreign nationals (Exhibit Z & Exhibit AA as an examples), and/or engages in nations deemed as adversaries according to Title 15, 791.4 - Determination of Foreign Adversaries, and Title 10 USC Section 4872(d)(2). In discussing the safety concerns revolving around Data Brokers, the GAO details the very same methodologies the above two groups cite in the Terms of Service and Privacy Policies to aggregate individuals' data through their collection of Personal Information and further amplification via consolidation of Publicly Available Information. The GAO report stresses;

“Emerging technological capabilities (such as artificial intelligence, machine learning, and data mining) have the potential to advance the continued aggregation and analysis of data on individuals' personal and professional lives. These technologies enhance the speed, accuracy, and ability to predict behavior across large data sets, but they also introduce a number of risks to DoD. Those risks include counterintelligence, force protection, safety and **security of family members**, insider threat, mission assurance, OPSEC (operational security) and program protection.” (Exhibit Y, page 8)

The identification of digital footprints posing security risks to military family members deserves specific attention. In the same GAO report, the Office of the Under Secretary of Defense for Intelligence and Security agreed the aggregation of digital footprints could have significant security implications and emphasized they had in fact seen family members targeted during deployments, while further acknowledging its adverse impact on mission. (Exhibit Y, page 14) With this in mind, while the above identified Data Broker companies state they are collecting such data to enable safety and fair play, they could be consolidating the very data that poses a security risk to the Department of Defense, military members and their families, to include their children. Additionally, the Data Broker companies supporting youth sports start collecting data on children as young as six, meaning such children could have highly detailed digital footprints of aggregated data covering the full details of their lives by the time they're old enough to serve in the U.S. military. As detailed in the GAO report, if such files are attained by foreign adversaries, they could be used as blackmail, targeting for particular vulnerabilities, or any plethora of other such weaknesses that could significantly adversely impact future DoD recruiting and accession efforts.

**SPECIFIC REQUESTS:** Due to the Federal Trade Commission's unique authority to enforce COPPA and prohibit unfair or deceptive acts, we respectfully request the Commission compel the Respondents and the youth sports data brokerage industry to comply with the following:

1. **Enforce 16 C.F.R. § 312.7 by Prohibiting Mandatory Digital IDs:** Issue an order declaring that the collection of biometric data, social media profiles, and permanent digital identifiers is not "reasonably necessary" for the activity of youth sports participation. Consequently, Respondents must be prohibited from conditioning eligibility on the creation of such accounts.
2. **Mandate "Opt-In" Privacy Defaults:** Require that any "Digital ID" or "Player Profile" service be offered strictly as a voluntary, opt-in product. The default method for age verification must remain a data-minimized, non-retention standard (e.g., physical document review) unless a parent affirmatively and expressly consents to the digital alternative for their own convenience.
3. **Prohibit "Pay-to-Play" Data Coercion:** Declare the practice of "profit sharing" between data brokers and sports leagues (where leagues are paid to mandate data collection) an unfair trade practice that effectively bypasses meaningful parental consent.
4. **Enforce Strict Data Minimization & Segregation:** Compel these companies to stop sharing children's PII with "third-party partners," affiliates, and foreign entities without a separate, uncoerced parental consent process that is distinct from the consent required to play the sport.
5. **National Security Review:** Given the potential exposure of sensitive data to foreign adversaries, as highlighted by the GAO, we urge the Commission to coordinate with national security agencies to review the data handling practices of these brokers regarding military families (both current and future).