



May 13, 2021

The Honorable Amy Klobuchar, Chair
The Honorable Mike Lee, Ranking Member
Senate Judiciary Committee Subcommittee on
Competition Policy, Antitrust, and Consumer Rights

Dear Chairwoman Klobuchar and Ranking Member Lee:

Thank you for the opportunity to testify about the App Store before the Subcommittee last month. I appreciate your leadership on antitrust issues, and I look forward to continuing to work with you to ensure that markets are competitive, innovation thrives, and consumers benefit.

At Apple, we're proud of the store we've built, the experience it has provided our customers, and the opportunities it has created for developers to build and distribute software. Apple created the App Store more than a decade ago, as an alternative to the open Internet, to afford developers the opportunity to provide native apps to customers. Because of the App Store, not only do developers have a safe and trusted marketplace through which they can reach customers around the world,¹ they also can leverage Apple's innovations, including its intellectual property, to build and improve their apps. As I testified at the Subcommittee's hearing, the App Store is not just the gallery in which developers can sell their apps, it's also a studio stocked with the tools they need to create those apps in the first place.

All of this has revolutionized and democratized software development. The result has been extraordinary, with the App Store supporting about 2.1 million American jobs and generating about \$138 billion in economic activity across all fifty states in 2019 alone. New apps built by small businesses are coming online every day, and we are confident that many will become engines of economic growth and spur increased competition.

The developers who testified at the hearing were among some of the largest and most successful on the App Store,² and their testimony was focused more on grievances related to business disputes with Apple than on competition concerns with the App Store. To ensure an accurate and complete record, I am writing to address some of the particular accusations and arguments that were levied against Apple by other witnesses during the hearing. Rather than demonstrating a problem with competition, these witnesses—representing companies that have thrived in Apple's ecosystem—showcased how Apple and the iOS ecosystem foster competition.

¹ As noted in the enclosed Apple Newsroom post, by screening apps, Apple protected customers from more than \$1.5 billion in potentially fraudulent transactions in 2020 alone—preventing the attempted theft of money, information, and time—and kept nearly a million risky and vulnerable new apps off customers' iPhones.

² Spotify, Tinder, and Tile—together with Epic Games—are among the founders and funders of the "Coalition for App Fairness."

SPOTIFY

Spotify is the #1 music streaming service in the world. It is valued at nearly \$45 billion dollars, and its app has been downloaded nearly 500 million times from the App Store. Spotify grew to its current position in part because of the opportunities and technologies provided by the App Store.

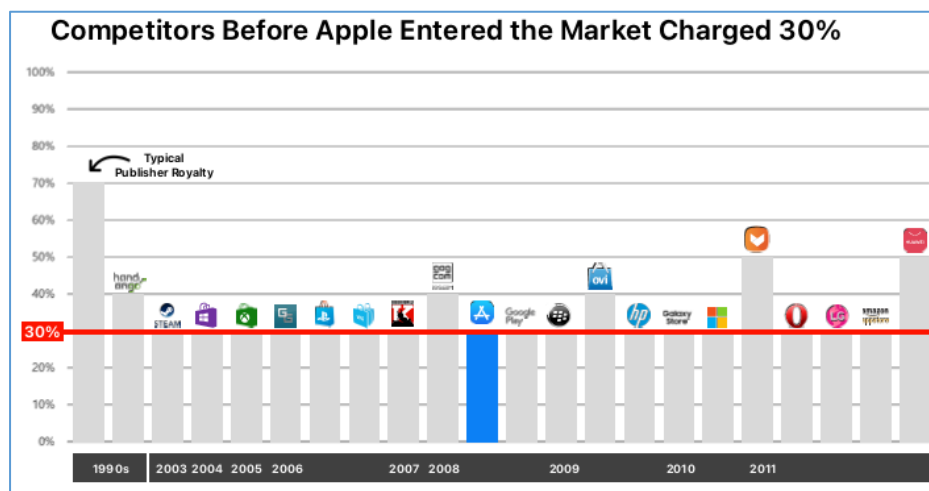
Spotify's witness made three central arguments during the hearing, each of which we dispute:

First, Spotify's witness argued that Apple's commission is too high and is not subject to competition. For example, he said: "[I]f Apple is convinced that their payment system is that superior, that it really should command a 30% fee, they should allow for competition and let the market determine that. Let supply and demand determine what the right fee is, but they haven't done that." In fact, however, **not only have market forces established a competitive commission, Apple meets or beats it.**

Before the App Store was launched, software distribution was difficult and expensive, often requiring fees of up to 70%. When Apple launched the App Store, we initially charged a 30% commission, thereby reducing barriers to entry for software developers.

Since then we have never raised the commission; we have only lowered it, including for subscriptions and small businesses, or we have eliminated it altogether in certain situations, as with the Reader Rule and the Multi-Platform Rule. Today, about 85% of apps pay no commission, and the vast majority of developers that do pay a commission can pay just 15% by entering our Small Business Program. The remainder—those making over \$1 million per year selling digital goods or services in the App Store—pay a 30% commission (which is reduced to 15% for subscription services after the first year). Spotify has benefited from this commission structure: it pays a commission on less than **one percent** of its premium subscribers, and that commission is always just 15%.³

Contrary to the Spotify witness' assertion at the hearing, the App Store commission is the result of market forces and intense competition. Spotify's own CEO has acknowledged as much, describing Spotify's "ubiquity" strategy as one whereby Spotify would be accessible by users on several major platforms. Given all those options, Apple has to compete to make the App Store an attractive option for developers. And we have done that: as shown here, even Apple's 30% commission meets or beats the rates charged by competitors. That commission reflects the value not just of distribution through the App Store, but also the suite of tools, technology, and intellectual property developers use to create, test, publish, and manage their apps.



³ When Apple reduced commissions applicable to Spotify, Spotify did not reduce its prices for its customers, notwithstanding Spotify's witness' testimony that "paying Apple's 30% tax . . . would have forced us to raise consumer prices."

Second, Spotify's witness stated: "Apple's anti-competitive intent is clear from the fact that [the App Store commission] targets businesses that are or might become Apple's competitors in downstream markets. The rules apply to companies that offer online gaming, music and video streaming, access to eBooks, but companies like Uber, Starbucks, Ticketmaster and Walmart, are exempt." In fact, however, **Apple consistently has, since the launch of the App Store, distinguished between (a) digital goods/services and (b) physical goods/services, a distinction that applies equally to all developers and reflects the added value enjoyed by sellers of digital goods/services.**

Apple charges a commission in just one situation: when a developer (1) makes a sale to a customer *in* the App Store and (2) sells that customer a product/service used *on* the iPhone. This distinction is similar to that made in other app stores—like those from Amazon, Google, and Samsung—and it makes sense:

- First, as with other stores, including brick-and-mortar stores, when a producer of a good/service makes a sale in the App Store, that sale may be subject to a commission; however, if the developer makes the sale outside the App Store (e.g., on its own website), no commission applies. As noted above, Spotify has benefitted from this distinction: the vast majority of its subscribers have signed-up for Spotify outside the App Store, and Spotify pays no commission in those circumstances.
- Second, whereas a physical good/service (like the ride you hail from Uber, the coffee you order from Starbucks, the concert you attend with tickets from Ticketmaster, or the couch you buy from Walmart) is experienced in the physical world, a digital good/service (like a sword you buy for your character in a video game or a show you stream on your iPhone) is experienced on your iPhone and relies most heavily upon the device's technologies, features, and intellectual property that are essential to the user's experience of the app.

This commission structure does not "target [] businesses that are or might become Apple's competitors," as Spotify's witness claimed at the hearing. For one thing, the distinction between digital and physical goods/services has been in place since the App Store was launched in 2008—*before* Apple began offering digital goods/services like Apple Music, Apple TV+, and Apple Books. In addition, many third-party apps that compete with Apple's own apps pay no commission, and many third-party apps that do not compete with Apple's own services do pay a commission, so the idea that the commission is based on competitive considerations is simply not borne out by the facts.

Third, Spotify's witness complained about what he described as "a gag order" prohibiting Spotify from communicating with its customers "about the existence of premium service, discounts, and promotions available to first-time subscribers." Spotify's witnesses appeared to allege that this was a "unilateral change" to the App Store "rules that retroactively outlawed things that [Spotify] did in [its] products."

In fact, however, **Apple does not prohibit developers from communicating with their customers; Apple simply says that developers cannot redirect customers who are in the App Store to leave the App Store and go elsewhere—just as Apple cannot put a sign in the Verizon store, telling customers to buy iPhones directly from Apple instead.** The rule is one that has long-been embraced by retailers in both the physical and digital worlds. As for Apple, this common-sense rule has been in place since 2009, pre-dating Spotify's launch on the App Store. Spotify launched, grew, and thrived under these rules, but now Spotify apparently either wants Apple to change them or to hold Spotify to a different set of standards from everyone else.

Finally, Spotify's witness made additional statements that Apple disputes. For example, he stated that "iPhones weren't that popular when first introduced" when, in fact, iPhone was named the 2007 Invention of the Year by Time Magazine, is widely acknowledged as one of the most innovative products in decades, and was so popular that Apple struggled to meet demand in early years. Spotify's witness also said that Apple made a "clear statement" that Spotify's app "would never be promoted on the App Store or receive [] any marketing because [Spotify was] a competitor." I am not aware of Apple ever having made any such statement, and we routinely promote apps that compete against our own, including Spotify and other music streaming services. Finally, Spotify's witness claimed that Apple had taken a "series of steps" "threatening to kick [Spotify] out of the App Store," but the issues he identified involved enforcement of the App Store's rules, which apply equally to all developers. Spotify's app has been available to users for download from the App Store without interruption.

MATCH/TINDER

Match has the largest U.S. market share of any company in the dating app space. It has acquired several companies, including would-be competitors, to establish itself as the market leader. Match generated more than \$2 billion in revenue in 2019, and its apps have enjoyed success across a variety of platforms, including iOS. Tinder is now the number one grossing app worldwide, and it has been successful in part by employing a "freemium" model through which users can enjoy many of its core features at no cost. Tinder does not pay Apple for the distribution of its app unless a user subscribes to Tinder's premium service—and even then, only if the user does so through the App Store.

Tinder's witness made a number of statements at the hearing with which we disagree. For example:

First, Tinder's witness conflated the App Store with the open Internet, describing the former as a "tollway[] on the formerly free information superhighway." In reality, **customers have lots of choices for accessing digital content, including the open Internet.** The App Store was never intended to replace the open Internet; rather, Apple created the App Store to afford developers an additional opportunity to reach customers by providing native apps in a safe and trusted marketplace. Tinder takes full advantage of this: it promotes "Tinder Online" as a way to access Tinder through its website on the open Internet, where users can buy subscriptions directly from Tinder and then use them on the app.

Second, Tinder's witness mischaracterized the nature of Apple's commission (which, as noted above, applies to about 15% of apps and typically is 15%) and Apple's in-app payment (IAP) system. IAP is not a "credit card processor," as Tinder's witness stated, and Apple's commission is not a processing fee. Rather, **Apple's commission reflects the value of the powerful technology platform, tools, software, curated marketplace, and intellectual property that allows developers to create and distribute apps.** In addition, IAP provides important consumer protections, like the "Ask to Buy" parental control feature, transparent pricing and terms, purchase history, subscription management, and other App Store features like Family Sharing.

Third, Tinder's witness claimed that Apple rejects apps without adequately explaining how the App Store's rules were violated or how to fix the issue. In fact, however, **Apple puts enormous effort into its communications with developers to help them get their apps into the App Store.** In each instance when an app is rejected, Apple identifies the specific App Store guideline with which the app does not comply and provides the factual basis that resulted in the rejection (often including relevant screenshots). If a developer has questions about a rejection, they have many options to reach out to the App Review team, including via email or phone. Indeed, Apple participates in about 1,000 calls a

week to developers to help them diagnose and resolve any issues that led to rejection, so they can get their app on the App Store.

Tinder's witness provided one purported example of this alleged problem—a safety feature for members of the LGBTQ+ community that, according to Tinder's witness, “sat in the App Store review process for two months because Apple had said that we were violating a new policy or they said the spirit of the policy and couldn't tell us expressly how we needed to solve it.” That is not accurate. Tinder submitted an update to Apple in June 2019 that included both an update to the app's subscription pricing and the “Traveler Alert” for members of the LGBTQ+ community. Apple explained that Tinder's new subscription pricing would violate FTC rules because Tinder did not make clear to customers that they would be charged for the full six-month subscription rather than a monthly charge. For one month (not two), Apple engaged in communications with Tinder, asking it to comply with fair consumer pricing rules and explaining that once changes to the description of subscription pricing were made, the updates would be approved. Tinder complied, and in July 2019 the updates, including the “Traveler Alert,” were approved. This is an example of Apple engaging in extensive discussions with a developer to ensure that the developer's app is made available to customers and that the App Store remains a safe and trusted place for consumers.

Finally, Tinder's witness claimed that Apple does not do enough to prevent underage users from downloading Tinder. However, **Apple strives to make the App Store a safe and trusted marketplace, including by empowering parents with parental controls.** If a parent doesn't want their child to have access to Tinder, for example, we have given them tools to deny that access. To the extent that Tinder wants Apple to share its customers' age data, that is prohibited by privacy laws and Apple's privacy policy. And to the extent that Tinder is having difficulty ensuring that its own users comply with its own policies, then Tinder should consider investing in better age-verification measures. If Tinder's users are entering false birthdates, blocking the download of an app will not fix the problem because the same users can easily access Tinder and enter a false birthdate when accessing Tinder elsewhere.

TILE

Tile describes itself on its website as “the largest, fastest and most powerful lost and found community in the world” with 80% of the U.S. retail market for item-tracking devices. Tile appears unhappy that new competition has emerged to challenge its dominance. Consumers can now choose between Tile, Samsung's SmartTags tracker, Chipolo item finders, and Apple's AirTags.

With AirTags, Apple innovated by bringing our commitment to privacy to offer a more secure, privacy-protected approach to item finding. AirTags was designed with privacy in mind, including end-to-end encryption and built-in protections to ensure that location data cannot be accessed by Apple or other third parties. And we implemented a new Ultra-Wide Band (UWB) technology to allow users to precisely pinpoint their item. Even Tile's CEO acknowledged in a recent interview that Tile's product is a “super differentiated product” from Apple's AirTags.

Even more competition is coming thanks to Apple's decision to provide free access to its secure and private Find My network, which will allow third-party device manufacturers to use Find My to offer item-tracking functionality, enabling even more competition. The program announced a month ago has already been adopted by Chipolo item finders, VanMoof bikes, and others.

Tile's witness made a number of statements with which we disagree, including the following:

First, Tile's witness took issue with some of the privacy protections that Apple offers its customers. For example, Tile's witness complained about privacy protections that purportedly "denigrated [Tile's] user experience and made it really hard for [its] customers to activate their Tiles." However, **at Apple, we believe that privacy is a fundamental human right, and we design all of our products and services with that in mind.** The privacy changes about which Tile's witness appeared to complain were notifications that help users better understand when their location data was being accessed by an app and to provide users greater control over whether or not to share that data with developers. The changes require all developers (not just Tile) to seek explicit user consent to access user location data, preventing them from continuously uploading users' location data, even when an app was not being used. These location prompts and settings apply to Apple's own apps.

Tile and other apps access sensitive user location data, collect it, and store it on their own servers. Apple does not do that. Rather, Find My only stores user location data locally on the user's iPhone, where it is inaccessible to Apple or anyone else except the user. Find My does not give customers notifications about location tracking in the same way as Tile because Apple is not collecting that data. It all happens on device unless the user is actively looking for his or her lost item. Apple competes on the merits and holds itself to the same or higher privacy standard as third-party apps.

Second, Tile's witness alleged that Apple has decided to reserve the use of UWB technology exclusively in Apple's product. However, **Apple constantly makes features, functionalities, and APIs available to third-parties for their own development**, and weeks ago, Apple publicly announced that a draft specification of UWB for chipset manufacturers will be released later this spring. To achieve this, Apple is now working with an industry consortium to make sure our UWB solution is compliant with open industry standards, and ensuring interoperability with a variety of different products. With this, third-party device makers will soon be able to take advantage of UWB in Apple devices. While Tile does not currently have a commercially available product that can take advantage of UWB, when they do develop such a product they will be able to use UWB because Apple is following these open industry standards. This is consistent with our practice of opening Apple-developed technologies to third-party developers once we are certain that they work without issue, and do not create security or data-privacy risks.

Third, Tile's witness testified that "[w]ith iOS 13, Apple introduced a new Find My app that had Tile features. That is basically their version of Tile." Find My was introduced by Apple in 2010—well before Tile was even founded—to help users remotely locate their Apple device, secure its data, or wipe its data. Tile was not founded until December 2012. And years later, in 2019 when iOS 13 was released, Apple added a limited new feature that would enable Find My to locate Apple devices when they were not connected to the Internet. This capability to locate iPhones and iPads was far removed from Tile's broader application to help its users find "millions" of "unique items every day."

Finally, Tile's witness claimed that Apple: "know[s] our retail take rates, they know our retail margins, they know how our devices do in stores, they know who our customers are, they know our subscription take rates[,] [and] [t]hey know what features people use." Years ago, Apple had some information about how Tile products sold in Apple's retail store. It did not sell well. Tile sells its products through dozens of retailers around the globe and its own website. Any information from Apple Store retail sales is both very limited and very outdated and likely no different from the information other brick-and-mortar stores have about products sold in those stores. Nonetheless, Apple has never used any of that information in any decisionmaking related to AirTags.

I appreciated the opportunity to appear before the Subcommittee last month, and I ask that the Subcommittee include this letter in the record to ensure that there is an accurate reflection of the facts considered, particularly regarding specific allegations made against Apple at the hearing. We share the Subcommittee's commitment to promoting competition and innovation, allowing developers to thrive, and supporting the success of great American ideas.

Respectfully,

A handwritten signature in black ink, appearing to read "Kyle Andeer", written in a cursive style.

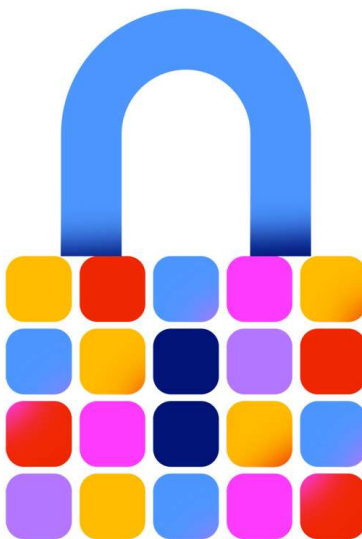
Kyle Andeer
Chief Compliance Officer

Enclosure

UPDATE

May 11, 2021

App Store stopped more than \$1.5 billion in potentially fraudulent transactions in 2020



Apple helps keep the App Store a safe and trusted place for users to discover apps by detecting and taking action against fraudulent developers and users.

Threats have been present since the first day the App Store launched on iPhone, and they've increased in both scale and sophistication in the years since. Apple has likewise scaled its efforts to meet those threats, taking relentless steps forward to combat these risks to users and developers alike.

It takes significant resources behind the scenes to ensure these bad actors can't exploit users' most sensitive information, from location to payment details. While it's impossible to catch every act of fraud or ill intent before it happens, thanks to

Apple's industry-leading antifraud efforts, security experts agree the App Store is the safest place to find and download apps.¹

In 2020 alone, Apple's combination of sophisticated technology and human expertise protected customers from more than \$1.5 billion in potentially fraudulent transactions, preventing the attempted theft of their money, information, and time — and kept nearly a million risky and vulnerable new apps out of their hands.



App Review

The App Review team is an essential line of defense, carefully reviewing every app and every update to ensure they adhere to the App Store's strong [guidelines](#) on privacy, security, and spam. The guidelines have changed over time to respond to new threats and challenges, with the goal of protecting users and providing them with the very best experience on the App Store.

Apple's goal is always to get new apps onto the store. In 2020, the team assisted more than 180,000 new developers in launching apps. Sometimes this takes a few tries. An app might be unfinished or not functioning properly when it's submitted for approval, or it might not yet have a sufficient mechanism for moderating user-generated content. In 2020, nearly 1 million problematic new

apps, and an additional nearly 1 million app updates, were rejected or removed for a range of reasons like those.

A smaller but significant set of these rejections was for egregious violations that could harm users or deeply diminish their experience. In 2020 alone, the App Review team rejected more than 48,000 apps for containing hidden or undocumented features, and more than 150,000 apps were rejected because they were found to be spam, copycats, or misleading to users in ways such as manipulating them into making a purchase.

Some developers perform a bait and switch: fundamentally changing how the app works after review to evade guidelines and commit forbidden and even criminal actions. When such apps are discovered, they're rejected or removed immediately from the store, and developers are notified of a 14-day appeals process before their accounts are permanently terminated. In 2020, about 95,000 apps were removed from the App Store for fraudulent violations, predominantly for these kind of bait-and-switch maneuvers.

In just the last few months, for example, Apple has rejected or removed apps that switched functionality after initial review to become real-money gambling apps, predatory loan issuers, and pornography hubs; used in-game signals to facilitate drug purchasing; and rewarded users for broadcasting illicit and pornographic content via video chat.

Another common reason apps are rejected is they simply ask for more user data than they need, or mishandle the data they do collect. In 2020, the App Review team rejected over 215,000 apps for those sorts of privacy violations. Apple believes privacy is a fundamental right, and this commitment is a major reason why users choose the App Store.

Even with these stringent review safeguards in place, with 1.8 million apps on the App Store, problems still surface. Users can report problematic apps by choosing the [Report a Problem](#) feature on the App Store or calling Apple Support, and developers can use either of those methods or additional channels like [Feedback Assistant](#) and [Apple Developer Support](#).

Fraudulent Ratings and Reviews

App Store ratings and reviews help many users make decisions about which apps to download, and developers rely on them to incorporate new features that respond to user feedback. Apple relies on a sophisticated system that combines machine learning, artificial intelligence, and human review by expert teams to moderate these ratings and reviews to help ensure accuracy and maintain trust. Since 2020, Apple has processed over 1 billion ratings and over 100 million reviews, and over 250 million ratings and reviews were removed for not meeting moderation standards.

Apple also recently deployed new tools to verify rating and review account authenticity, to analyze written reviews for signs of fraud, and to ensure that content from deactivated accounts is removed.

Account Fraud

Unfortunately, sometimes developer accounts are created entirely for fraudulent purposes. If a developer violation is egregious or repeated, the offender is expelled from the Apple Developer Program and their account terminated. Apple terminated 470,000 developer accounts in 2020 and rejected an additional 205,000 developer enrollments over fraud concerns, preventing these bad actors from ever submitting an app to the store.

Despite fraudsters' sophisticated techniques to obscure their actions, Apple's aggressive monitoring means these accounts are terminated, on average, less than a month after they are created.

Apple's work to ensure the safety of users who download apps extends even beyond the App Store. Over the last 12 months, Apple found and blocked nearly 110,000 illegitimate apps on pirate storefronts. These storefronts distribute malicious software often designed to resemble popular apps — or that modify popular apps without their developers' authorization — while circumventing the App Store's security protections.

And in just the last month, Apple blocked more than 3.2 million instances of apps distributed illicitly through the Apple Developer Enterprise Program. The program is designed to allow companies and other large organizations to develop and privately distribute internal-use apps to their employees that aren't available to the general public. Fraudsters attempt to distribute apps via this method to circumvent the rigorous App Review process, or to implicate a legitimate enterprise by manipulating an insider to leak credentials needed to ship illicit content.

In addition to fraudulent developer accounts, Apple works to identify and deactivate fraudulent user accounts. In 2020 alone, Apple deactivated 244 million customer accounts due to fraudulent and abusive activity. In addition, 424 million attempted account creations were rejected because they displayed patterns consistent with fraudulent and abusive activity.

Payment and Credit Card Fraud

Financial information and transactions are some of the most sensitive data that users share online. Apple has invested significant resources in building more secure payment technologies like Apple Pay and StoreKit, which are used by more than 900,000 apps to sell goods and services on the App Store. For example, with Apple Pay, credit card numbers are never shared with merchants — eliminating a risk factor in the payment transaction process.

With online data breaches frustratingly common, these protections are an essential part of keeping users safe. But users may not realize that when their credit card information is breached or stolen from another source, fraudsters may turn to online marketplaces like the App Store to attempt to purchase digital goods and services that can be laundered or used for illicit purposes.

Apple focuses relentlessly on this kind of fraud as well. In 2020 alone, the fusion of sophisticated technology and human review prevented more than 3 million stolen cards from being used to purchase stolen goods and services, and banned nearly 1 million accounts from transacting again. In total, Apple protected users from more than \$1.5 billion in potentially fraudulent transactions in 2020.

From App Review, to fraudulent account detection, to prevention of financial crimes, Apple works around the clock and behind the scenes to keep the App Store a safe and trusted place for users and developers alike.

Share article



1. nokia.com/networks/portfolio/cyber-security/threat-intelligence-report-2020; media.defense.gov

Press Contacts

Katie Clark Alsadder

Apple
kclarkalsadder@apple.com
(408) 974-9976

Fred Sainz

Apple
sainz@apple.com
(669) 227-0492

Apple Media Helpline

media.help@apple.com
(408) 974-2042

Latest Articles

UPDATE

Coders, designers, and entrepreneurs thrive thanks to Apple Developer Academy

May 12, 2021

The latest news and updates, direct from Apple.

[Read more >](#)

Newsroom		App Store stopped over \$1.5 billion in suspect transactions in 2020		
Shop and Learn		Services	Apple Store	For Business
Mac		Apple Music	Find a Store	Apple and Business
iPad		Apple TV+	Shop Online	Shop for Business
iPhone		Apple Fitness+	Genius Bar	For Education
Watch		Apple News+	Today at Apple	
TV		Apple Arcade	Apple Camp	
				Apple Values
				Accessibility
				Education
				Environment
				Inclusion and Diversity
				Privacy

Music	iCloud	Apple Store App	Shop for K-12	Racial Equity and Justice
AirPods	Apple One	Refurbished and Clearance	Shop for College	Supplier Responsibility
HomePod	Apple Card	Financing		
iPod touch	Apple Books	Apple Trade In	For Healthcare	About Apple
Accessories	App Store	Order Status	Apple in Healthcare	Newsroom
Gift Cards		Shopping Help	Health on Apple Watch	Apple Leadership
	Account		Health Records on iPhone	Job Opportunities
	Manage Your Apple ID			Investors
	Apple Store Account		For Government	Events
	iCloud.com		Shop for Government	Contact Apple
			Shop for Veterans and Military	

More ways to shop: [Find an Apple Store](#) or [other retailer](#) near you. Or call 1-800-MY-APPLE.