Published June 2024

Legal Process Guidelines

Government & Law Enforcement within the United States

These guidelines are provided for use by government and law enforcement agencies within the United States when seeking information from Apple Inc. ("Apple") about customers of Apple's devices, products and services. Apple will update these Guidelines as necessary.

All other requests for information regarding Apple customers, including customer questions about information disclosure, should be directed to https://www.apple.com/privacy/contact/. These Guidelines do not apply to requests made by government and law enforcement agencies outside the United States to Apple's relevant local entities.

For government and law enforcement information requests, Apple complies with the laws pertaining to global entities that control our data and we provide details as legally required. For all requests from government and law enforcement agencies within the United States for content, with the exception of emergency circumstances (defined in the Electronic Communications Privacy Act 1986, as amended), Apple will only provide content in response to a search warrant issued upon a showing of probable cause, or customer consent.

All requests from government and law enforcement agencies outside of the United States for content, with the exception of emergency circumstances (defined below in Emergency Requests), must comply with applicable laws, including the United States Electronic Communications Privacy Act (ECPA). A request under a Mutual Legal Assistance Treaty or the Clarifying Lawful Overseas Use of Data Act ("CLOUD Act") is in compliance with ECPA. Apple will provide customer content, as it exists in the customer's account, only in response to such legally valid process.

For private party requests, Apple complies with the laws pertaining to customer data and provides data as legally required.

Apple has a centralized process for receiving, tracking, processing, and responding to legitimate legal requests from government, law enforcement, and private parties from when they are received until when a response is provided. A trained team in our legal department reviews and evaluates all requests received, and requests which Apple determines to have no valid legal basis or considers to be unclear, inappropriate or over-broad are objected, challenged or rejected.

Apple provides responses to the requesting law enforcement agency at the official law enforcement email address of the requesting officer. All evidence preservation pursuant to the responses provided by Apple is the responsibility of the requesting law enforcement agency.

INDEX

I. General Information

Apple designs, manufactures, and markets mobile communication and media devices, personal computers, portable digital music players, and sells a variety of related software, services, peripherals, networking solutions, and third-party digital content and applications. Apple's products and services include Mac, iPhone, iPad, iPod touch, Apple TV, Apple TV+, Apple Watch, HomePod, AirPods, AirTag, a portfolio of consumer and professional software applications, the iOS and macOS X operating systems, iCloud, and a variety of accessory, service and support offerings. Apple also sells and delivers digital content and applications through Apple Music, App Store, Apple Books, and Mac App Store. Customer information is held by Apple in accordance with Apple's privacy policy and the applicable terms of service for the particular service offering. Apple is committed to maintaining the privacy of the customers of Apple products and services ("Apple customers"). Accordingly, other than in emergency situations as provided by law, information about Apple customers will not be released without valid legal process.

The information contained within these Guidelines is devised to provide information to government and law enforcement agencies within the United States regarding the legal process that Apple requires in order to disclose electronic information to government and law enforcement agencies within the United States. These Guidelines are not intended to provide legal advice. The frequently asked questions ("FAQ") section of these Guidelines is intended to provide answers to some of the more common questions that Apple receives. Neither these Guidelines nor the FAQ will cover every conceivable circumstance that may arise.

If you have further questions, please contact lawenforcement@apple.com.

The above mailbox is intended solely for use by law enforcement and government personnel. If you choose to send an email to this address, it must be from a valid and official government or law enforcement email address.

Subpoenas, search warrants, and court orders that law enforcement submits to Apple should seek information regarding a particular Apple device or customer and the specific service(s) that Apple may provide to that customer. Apple can provide Apple device or customer information in so far as Apple still possesses the requested information pursuant to its data retention policies. Apple retains data as outlined in certain "Information Available" sections below. All other data is retained for the period necessary to fulfill the purposes outlined in our privacy policy. Apple believes that privacy is a fundamental human right and Apple implements that belief through not only its products and services but its law enforcement response guidelines as well. Additionally, Apple expects that before serving legal process, law enforcement will ensure that their investigations are lawful and respectful of civil rights. To the extent Apple observes patterns and practices that suggest civil rights abuses may be occurring, Apple will review challenging any associated law enforcement legal process. Government and law enforcement agencies should be as narrow and specific as possible when fashioning their legal process to avoid misinterpretation, objection, challenge and/or rejection in response to an unclear, inappropriate, or over-broad request. With the exception of emergency circumstances (defined in the Electronic Communications Privacy Act 1986, as amended) and situations in which a customer has consented, a search warrant issued upon a probable cause showing is required when government and law enforcement are requesting customer content.

Nothing within these Guidelines is meant to create any enforceable rights against Apple, and Apple's policies may be updated or changed in the future without further notice to government or law enforcement.

II. Service of Legal Process

A. Government, Law Enforcement, and Private Party Subpoenas, Search Warrants, and Court Orders

Apple accepts service of legal process by email to lawenforcement@apple.com from government and law enforcement agencies, provided it is transmitted from the official email address of the requesting agency.

To help ensure the legal process Apple receives is in the form and substance the issuing authority authorized, Apple requires submission of the complete legal process, including attachments, in an uneditable PDF.

Please Note: When legal process contains 5 or more search parameters, please include the search parameters in an editable document such as Numbers, Excel, Pages or Word. Apple will not download legal process documents through any links provided in an email due to system security standards. Additionally, providing a link to download the legal process will not be considered valid service of process.

For data security purposes, when the legal process contains full credit, debit, DPAN or Apple gift card numbers, the complete legal process and 5 or more search parameters should be transmitted in password-protected documents and the password transmitted in a separate email.

When government or law enforcement serve legal process on Apple by email to lawenforcement@apple.com, there is no need to serve a paper copy by mail.

Note: All legal requests that are not made by a government or law enforcement agency must be either personally served at Apple's headquarters: 20705 Valley Green Drive, Cupertino, California, 95014; or served through CT Corporation (Apple's registered agent for service of process).

For inquiries related to law enforcement legal process, please contact: lawenforcement@apple.com. If you are inquiring regarding the status of a specific subpoena, search warrant, or court order, please allow 10 business days after service of your request unless the matter involves imminent harm or threat to life.

B. Managing and Responding to Government, Law Enforcement, and Private Party Subpoenas, Search Warrants, and Court Orders

Apple carefully reviews all legal requests to ensure that there's a valid legal basis for each request, and complies with legally valid requests. Where Apple determines that there is no valid legal basis or where a request is considered to be unclear, inappropriate or over-broad, Apple will object, challenge or reject the request.

For processing purposes and due to system limitations, Apple cannot accept legal process that contains requests related to more than 25 identifiers. If law enforcement submits legal process with more than 25 identifiers, Apple will respond to the first 25 and law enforcement will need to resubmit new legal process for any additional identifiers.

C. Witness Testimony Subpoenas

Apple will not waive service requirements for subpoenas seeking witness testimony nor accept service via electronic means. All subpoenas seeking witness testimony must either be personally served on Apple or served through Apple's registered agent for service of process. Apple will resist subpoenas for witness testimony that are served with fewer than 14 days advance notice.

D. Preservation Requests

Requests to preserve information pursuant to 18 U.S.C. §2703(f) should be transmitted directly from an official government or law enforcement email address to lawenforcement@apple.com.

Preservation requests must include the relevant Apple ID/account email address, or full name **and** phone number, and/or full name **and** physical address of the customer of the subject Apple account. When a preservation request has been received, Apple will preserve a one-time data pull of the requested existing customer data available at the time of the request for 90 days. After this 90 day period, the preservation will be automatically removed from the storage server. However, this period can be extended for one additional 90-day period upon receipt of a renewed request. An attempt to serve more than two preservation requests for the same account will result in the second request being treated as a request for an extension of the original preservation, and not a separate preservation of new data. Requests for initiations of new preservations of data should be separately submitted, and must not be combined with requests for extensions of existing preservations.

E. Emergency Requests

The Electronic Communications Privacy Act ("ECPA") governs the authorized disclosure of data, including customer content, by Apple. An exception to the requirement that government or law enforcement obtain a search warrant for customer content is provided by ECPA in situations in which the case involves an emergency. Under 18 U.S.C. §§2702(b)(8) and 2702(c)(4), Apple is permitted, but not required, to voluntarily disclose information, including contents of communications and customer records, to a federal, state, or local governmental entity if Apple believes in good faith that an emergency involving imminent danger of death or serious physical injury to any person requires such disclosure without delay.

In order to request that Apple voluntarily disclose information on an emergency basis, the requesting government or law enforcement officer should complete the Emergency Government & Law Enforcement Information Request form and transmit it directly from their official government or law enforcement email address to exigent@apple.com with the words "Emergency Request" in the subject line.

If a government or law enforcement agency seeks customer data in response to an Emergency Government & Law Enforcement Information Request, a supervisor for the government or law enforcement agent who submitted the Emergency Government & Law Enforcement Information Request may be contacted and asked to confirm to Apple that the emergency request was legitimate. The government or law enforcement agent who submits the Emergency Government & Law Enforcement Information Request should provide the supervisor's contact information in the request.

If a government or law enforcement agency needs to contact Apple after hours (before 8:00 am or after 5:00 pm Pacific time) for an emergency inquiry, please contact Apple's Global Security Operations Center (GSOC) at (408) 974-2095.

F. Account Restriction/Deletion Requests

If a government or law enforcement agency, or private party requests that Apple restrict/delete a customer's Apple ID, Apple requires a court order (often a judgment of conviction or warrant) demonstrating the account to be restricted/deleted was used unlawfully.

Apple carefully reviews all requests from government, law enforcement and private parties to ensure there's a valid legal basis for each request. In instances where Apple determines there is no valid legal basis or where the court order does not demonstrate that the account to be restricted/deleted was used unlawfully, Apple will reject/challenge the request.

Where Apple receives a satisfactory court order (often a judgment of conviction or warrant) from government, law enforcement or private party demonstrating that the account to be restricted/deleted was used unlawfully, Apple will take the requisite action to restrict/delete the account in compliance with the court order; and advise the requesting agent/party accordingly.

G. Customer Notice

Apple will notify customers when their Apple account information is sought in response to legal process from government, law enforcement, or third parties, with the following exceptions:

Where providing notice is explicitly prohibited by the legal process itself, by a court order Apple receives (e.g., an order under 18 U.S.C. §2705(b)), by applicable law.

Where Apple, in its sole discretion, believes that providing notice creates a risk of injury or death to an identifiable individual, in child endangerment cases, or where notice is not applicable to the underlying facts of the case.

In emergency disclosure cases, Apple will provide delayed notice after the expiration of 90 days, unless the emergency disclosure relates to one of the exceptions referenced above.

Where notice is prohibited by a court order for a specific period of time, Apple will delay notice to the customer until after the expiration of the non-disclosure period specified in the court order. Notice will not be provided if the case relates to one of the exceptions referenced above.

In cases where customer accounts have been restricted/deleted as a result of Apple receiving a court order (often a judgment of conviction or warrant) demonstrating that the account to be restricted/deleted was used unlawfully or in violation of Apple's terms of service, Apple will notify its customers. Notice will not be provided if the case relates to one of the exceptions referenced above.

If Apple receives a National Security Letter (NSL) from the U.S. government that contains an indefinite gag order, Apple will notify the government that it would like the court to review the nondisclosure provision of the NSL pursuant to the USA FREEDOM Act of 2015. The government then has 30 days

to let the court know why the nondisclosure should remain in effect or can let Apple know that the nondisclosure no longer applies. If Apple receives notice that the nondisclosure no longer applies, it will notify the affected customer(s) pursuant to Apple's customer notice policies.

III. Information Available from Apple

This section covers the general types of information which may be available from Apple at the time of the publishing of these Guidelines.

A. Device Registration

Basic registration or customer information, including, name, address, email address, and telephone number is provided to Apple by customers when registering an Apple device prior to iOS 8 and macOS Sierra 10.12. Apple does not verify this information, and it may not be accurate or reflect the device's owner. Registration information for devices running iOS 8 and later versions, as well as Macs running macOS Sierra 10.12 and later versions is received when a customer associates a device to an iCloud Apple ID. This information may not be accurate or reflect the device's owner. Registration information, if available, may be obtained with a subpoena or greater legal process.

Please note, Apple device serial numbers do not contain the letters "O" or "I," rather Apple utilizes the numbers 0 (zero) and 1 (one) in serial numbers. Requests for serial numbers with either the letter "O" or "I" will yield no results.

B. Customer Service Records

Contacts that customers have had with Apple customer service regarding a device or service may be obtained from Apple. This information may include records of support interactions with customers regarding a particular Apple device or service. Additionally, information regarding the device, warranty, and repair may also be available. This information, if available, may be obtained with a subpoena or greater legal process.

C. Apple Media Services

App Store, Apple Music, Apple TV app, Apple Podcasts, and Apple Books ("Apple Media Services") are software applications which customers use to organize and play apps, digital music and video, and stream content. Apple Media Services also provide content for customers to download for their computers and iOS devices. When a customer opens an Apple account, basic customer information such as name, physical address, email address, and telephone number can be provided by the customer. Additionally, information regarding Apple Media Service purchase/download transactions and connections, update/re-download connections may also be available. IP address information may be limited to the most recent 18 months. Apple customer information and connection logs with IP addresses can be obtained with a subpoena or greater legal process. Apple Media Service purchase/download transactional records and records of the specific content purchased or downloaded, if available, may be obtained with an order under 18 U.S.C. §2703(d), or a court order with the equivalent legal standard, or a search warrant.

Requests for Apple Media Service data must include the Apple device identifier (serial number, IMEI, MEID, or GUID) or relevant Apple ID/account email address. If the Apple ID/account email address are unknown, it is necessary to provide Apple with Apple Media Service customer information in the form

of full name **and** phone number, and/or full name **and** physical address in order to identify the subject Apple account. Government or law enforcement officers may also provide a valid Apple Media Service order number or a complete debit or credit card number associated with the Apple Media Service purchase(s). A customer name in combination with these parameters may also be provided, but customer name alone is insufficient to obtain information.

Please note: For data security purposes, when the legal process contains full credit, debit, DPAN or Apple gift card numbers, the complete legal process, including attachments, should be transmitted in a password-protected uneditable PDF and the password transmitted in a separate email. When legal process contains 5 or more search parameters, please include the search parameters in a password-protected editable document such as Numbers, Excel, Pages or Word. Apple will not download legal process documents through any links provided in an email due to system security standards. Additionally, providing a link to download the legal process will not be considered valid service of process.

D. Apple Store Transactions

Point of Sale transactions are cash, credit/debit card, or gift card transactions that occur at an Apple Store. Requests for Point of Sale records must include the complete credit/debit card number used and may also include additional information such as date and time of transaction, amount, and items purchased. Information regarding the type of card associated with a particular purchase, name of the purchaser, email address, date/time of the transaction, amount of the transaction, and store location, if available, may be obtained with a subpoena or greater legal process.

Requests for duplicate copies of receipts must include the retail transaction number associated with the purchase(s) and, if available, they may be obtained with a subpoena or greater legal process.

Please note: For data security purposes, when the legal process contains full credit, debit, DPAN or Apple gift card numbers, the complete legal process, including attachments, should be transmitted in a password-protected uneditable PDF and the password transmitted in a separate email. When legal process contains 5 or more search parameters, please include the search parameters in a password-protected editable document such as Numbers, Excel, Pages or Word. Apple will not download legal process documents through any links provided in an email due to system security standards. Additionally, providing a link to download the legal process will not be considered valid service of process.

E. Apple.com Orders

Apple maintains information regarding orders online at Apple.com, which may include name of the purchaser, shipping address, telephone number, email address, product(s) purchased, purchase amount, and IP address of the purchase. Requests for information pertaining to orders online at Apple.com must include a complete credit/debit card number or an order number, or serial number of the item purchased. A customer name in combination with these parameters may also be provided, however customer name alone is insufficient to obtain information. Alternatively, requests for information pertaining to orders online at Apple.com may include the relevant Apple ID/account email address. If the Apple ID/account email address are unknown, Apple requires customer information in the form of full name **and** phone number, and/or full name **and** physical address to identify the subject Apple account. Purchase information for orders online at Apple.com, if available, may be obtained with a subpoena or greater legal process.

Please note: For data security purposes, when the legal process contains full credit, debit, DPAN or Apple gift card numbers, the complete legal process, including attachments, should be transmitted in a password-protected uneditable PDF and the password transmitted in a separate email. When legal process contains 5 or more search parameters, please include the search parameters in a password-protected editable document such as Numbers, Excel, Pages or Word. Apple will not download legal process documents through any links provided in an email due to system security standards. Additionally, providing a link to download the legal process will not be considered valid service of process.

F. Gift Cards

Apple Store Gift Cards, App Store & iTunes Gift Cards, and Apple Gift Cards have a serial number. These serial numbers have multiple formats depending on variables such as design and/or date of issue. Apple may provide available information regarding Apple Store Gift Cards, App Store & iTunes Gift Cards, and Apple Gift Cards in response to a subpoena or greater legal process.

i. Apple Store Gift Cards

Apple Store Gift Cards may be used for purchases in either Apple.com or an Apple Store. Available records may include gift card purchaser information (if purchased from Apple as opposed to a third-party merchant), associated purchase transactions, and items purchased. In some instances, Apple may be able to cancel or suspend an Apple Store Gift Card, depending on the status of the specific card. Apple Store Gift Card information, if available, may be obtained with a subpoena or greater legal process.

Please note: For data security purposes, when the legal process contains full credit, debit, DPAN or Apple gift card numbers, the complete legal process, including attachments, should be transmitted in a password-protected uneditable PDF and the password transmitted in a separate email. When legal process contains 5 or more search parameters, please include the search parameters in a password-protected editable document such as Numbers, Excel, Pages or Word. Apple will not download legal process documents through any links provided in an email due to system security standards. Additionally, providing a link to download the legal process will not be considered valid service of process.

ii. App Store & iTunes Gift Cards

App Store & iTunes Gift Cards can be used in Apple Music, App Store, Apple Books and Mac App Store. With the serial number, Apple can determine whether the App Store & iTunes Gift Card has been activated (purchased at a retail point-of-sale) or redeemed (added to the store credit balance of an Apple account).

When an App Store & iTunes Gift Card is activated, available records may include the name of the store, location, date, and time. When an App Store & iTunes Gift Card is redeemed, available records may include customer information for the related Apple account, date and time of activation and/or redemption, and redemption IP address. In some instances, Apple may be able to disable an App Store & iTunes Gift Card, depending on the status of the specific card. App Store & iTunes Gift Card information, if available, may be obtained with a subpoena or greater legal process.

Please note: For data security purposes, when the legal process contains full credit, debit, DPAN or Apple gift card numbers, the complete legal process, including attachments, should be transmitted in a password-protected uneditable PDF and the password transmitted in a separate email. When legal process contains 5 or more search parameters, please include the search parameters in a password-protected editable document such as Numbers, Excel, Pages or Word. Apple will not download legal process documents through any links provided in an email due to system security standards. Additionally, providing a link to download the legal process will not be considered valid service of process.

iii. Apple Gift Cards

Apple Gift Cards can be used in the U.S. for purchasing everything Apple — products, accessories, apps, games, music, movies, TV shows, subscriptions, iCloud, and more — all in one card. The Apple ID balance is now the Apple Account Balance and can be used for any Apple product or service. Apple Gift Card can also be brought to a retail location to redeem in person. Apple Gift Card information, if available, may be obtained with a subpoena or greater legal process.

Please note: For data security purposes, when the legal process contains full credit, debit, DPAN or Apple gift card numbers, the complete legal process, including attachments, should be transmitted in a password-protected uneditable PDF and the password transmitted in a separate email. When legal process contains 5 or more search parameters, please include the search parameters in a password-protected editable document such as Numbers, Excel, Pages or Word. Apple will not download legal process documents through any links provided in an email due to system security standards. Additionally, providing a link to download the legal process will not be considered valid service of process.

G. Apple Cash

Apple Cash, which includes the ability to send and receive money person to person with Messages and the Apple Cash Card, is a service provided by Green Dot Bank, a Utah state chartered bank, Member FDIC. Green Dot Bank offers and operates Apple Cash, is responsible for customers and their transactions, and maintains all associated information. Apple does not keep any transactional records related to Apple Cash. Accordingly, requests for Apple Cash information should be directed to Green Dot Bank.

Service of legal process should be sent to Fax: 866.963.6235 or Mail: Green Dot Bank, P.O. Box 5100, Pasadena, CA 91117. Inquiries may be emailed to: ApplePayCashLawEnforcementSupport@greendotcorp.com.

H. Apple Pay

Apple Pay transactions made at retail locations (e.g., for NFC/contactless communications) and in apps or online points-of-sale are authenticated securely on the customer's device and sent in encrypted form to the merchant or the merchant's payment processor. While transaction security is verified by an Apple server, Apple does not process payments or store such transactions nor the full credit/debit card numbers associated with purchases made using Apple Pay. This information may be available through the relevant issuing bank, the payment network, or the merchant.

To request transactional data for Apple Pay purchases made at Apple Store locations or through Apple.com, Apple requires the Device Primary Account Number (DPAN) used for the transaction. The DPAN is 16 digits and can be obtained from the issuing bank. Note: The DPAN is used in contactless payment transactions with the merchant in place of the actual credit/debit card number (FPAN/Funding PAN). The DPAN is converted into the corresponding FPAN by the payment processor. With the relevant DPAN information, Apple may be able to conduct a reasonable search to locate responsive information through its point-of-sale system. These records, if available, may be obtained with a subpoena or greater legal process.

Apple may be able to provide Apple Pay information regarding the type(s) of credit/debit card(s) a customer has added to Apple Pay along with customer information. This information, if available, may be obtained with a subpoena or greater legal process. To request such information, Apple would require a device identifier (Apple serial number, SEID, IMEI or MEID); or an Apple ID/account email address.

Please note: For data security purposes, when the legal process contains full credit, debit, DPAN or Apple gift card numbers, the complete legal process, including attachments, should be transmitted in a password-protected uneditable PDF and the password transmitted in a separate email. When legal process contains 5 or more search parameters, please include the search parameters in a password-protected editable document such as Numbers, Excel, Pages or Word. Apple will not download legal process documents through any links provided in an email due to system security standards. Additionally, providing a link to download the legal process will not be considered valid service of process.

I. Apple Pay Later

Apple Pay Later is offered by Apple Financing LLC, a wholly owned subsidiary of Apple Inc. As the finance provider of Apple Pay Later loans, Apple Financing LLC maintains records related to the Apple Pay Later program. Accordingly, legal process seeking information related to Apple Pay Later should be directed to Apple Financing LLC and be sent to lawenforcement@apple.com.

Apple Pay Later is available in the U.S. for online and in-app purchases on iPhone or iPad with iOS or iPadOS 16.4 or greater. Apple Pay Later provides eligible U.S. users with the ability to split the cost of an Apple Pay purchase into four substantially equal payments over six weeks with no interest and no fees. Users can apply for Apple Pay Later loans of $50 - $1,000. Eligible users will see the Pay Later option when they select Apple Pay at checkout online and in-app. To complete a purchase transaction with Apple Pay Later, a user must use an Apple Pay provisioned debit card for the down payment. Subsequent Apple Pay Later loan repayments may be completed using an Apple Pay-eligible debit card or Apple Cash. Apple Pay Later transactions made online or in-app are authenticated securely on the customer's device and sent in encrypted form to the merchant or the merchant's payment processor.

Apple Financing LLC may be able to provide Apple Pay Later information regarding a customer's Apple Pay Later application, loan, or loan repayment. This information, if available, may be obtained with a subpoena or greater legal process. To request such information, please submit legal process directed to Apple Financing LLC which includes:

1) 12 digit Apple Pay Later Loan ID **and** date of transaction(s); and/or
2) Primary Account Number (PAN); and/or
3) Network Transaction ID **and** date of transaction(s); and/or
4) Apple ID/account email address; and/or
5) full name **and** phone number; and/or

6) full name **and** physical address; and/or
7) full name, social security number **and** date of birth.

For data security purposes, when your legal process contains a PAN number, the PAN number should be transmitted in a password-protected document (.PDF and editable format, example Numbers, Excel, Pages or Word document) to lawenforcement@apple.com and the password should be transmitted in a separate email.

Apple Inc. may be able to provide Apple Pay Later information related to limited Apple Pay Later customer support interactions. This information, if available, may be obtained with a subpoena or greater legal process. To request such information, please submit separate legal process directed to Apple Inc. which includes:

1) Apple ID/account email address; and/or
2) full name **and** phone number; and/or
3) full name **and** physical address.

J. Apple Card

Apple Card is a credit card created by Apple. Goldman Sachs Bank USA, Salt Lake City Branch, is the issuing bank for Apple Card. Goldman Sachs manages Apple Card and associated financial transactions, and maintains associated records. Apple does not keep any records related to Apple Card financial transactions. Accordingly, as the issuing bank and regulated financial institution responsible for managing Apple Card and related financial transactions, requests for information related to Apple Card transactions should be directed to Goldman Sachs. The Goldman Sachs support line for questions is: 877-255-5923.

K. Savings

Goldman Sachs Bank USA, Salt Lake City Branch, is the providing bank for Savings. Goldman Sachs manages Savings and associated financial transactions and maintains associated records. Apple does not keep any such records. Accordingly, as the providing bank responsible for Savings, requests for information should be directed to Goldman Sachs. The Goldman Sachs support line for questions is: 877-255-5923.

L. iCloud

iCloud is Apple's cloud service that allows customers to access their photos, documents, and more from all their devices. iCloud also enables customers to back up their iOS or iPadOS devices to iCloud. With iCloud, customers can set up an iCloud.com email account. iCloud email domains can be @icloud.com, @me.com and @mac.com. All iCloud content data stored by Apple is additionally encrypted at the location of the server. For data Apple can decrypt, Apple retains the encryption keys in its U.S. data centers. Apple does not receive or retain encryption keys for customer's end-to-end encrypted data.

iCloud is a customer based service. Requests for iCloud data must include the relevant Apple ID/account email address. If the Apple ID/account email address are unknown, Apple requires customer information in the form of full name and phone number, and/or full name and physical address to identify the subject Apple account. Where only an Apple ID/account email address are provided, available information for verified accounts associated with these criteria may be produced. Where only

a phone number is provided, only currently registered FaceTime, iMessage, or security verified phone numbers may be produced.

I. The following information may be available from iCloud:

a. Customer Information

When a customer sets up an iCloud account, basic customer information such as name, physical address, email address, and telephone number may be provided to Apple. Additionally, information regarding iCloud feature connections may also be available. iCloud customer information and connection logs with IP addresses, if available, may be obtained with a subpoena or greater legal process. Connection logs are retained up to 25 days.

b. Mail Logs

Mail logs include records of incoming and outgoing communications such as time, date, sender email addresses, and recipient email addresses. Mail logs, if available, may be obtained with a court order under 18 U.S.C. §2703(d), or a court order with an equivalent legal standard, or a search warrant. iCloud mail logs are retained up to 25 days.

c. Email Content and Other iCloud Content, My Photo Stream, iCloud Photo Library, iCloud Drive, Contacts, Calendars, Bookmarks, Safari Browsing History, Maps Search History, Messages, iOS Device Backups

iCloud stores content for the services that the customer has elected to maintain in the account while the customer's account remains active. Apple does not retain deleted content once it is cleared from Apple's servers. iCloud content may include email, stored photos, documents, contacts, calendars, bookmarks, Safari Browsing History, Maps Search History, Messages and iOS device backups. iOS device backups may include photos and videos in the Camera Roll, device settings, app data, iMessage, Business Chat, SMS, and MMS messages and voicemail. For data Apple can decrypt, Apple retains the encryption keys in its U.S. data centers. Apple does not receive or retain encryption keys for customer's end-to-end encrypted data. iCloud content, as it exists in the customer's account, may be provided in response to a search warrant issued upon a showing of probable cause, or customer consent.

II. **Advanced Data Protection**

Advanced Data Protection for iCloud is a feature that uses end-to-end encryption to protect iCloud data with Apple's highest level of data security. For users who enable Advanced Data Protection for iCloud, limited iCloud data may be available. More information on Advanced Data Protection can be found at: https://support.apple.com/kb/HT212520

The following information may be available from iCloud if a user has enabled Advanced Data Protection for iCloud:

a. Customer Information

When a customer sets up an iCloud account, basic customer information such as name, physical address, email address, and telephone number may be provided to Apple. Additionally, information regarding iCloud feature connections may also be available. iCloud customer information and connection logs with IP addresses, if available, may be obtained with a subpoena or greater legal process. Connection logs are retained up to 25 days.

b. Mail Logs

Mail logs include records of incoming and outgoing communications such as time, date, sender email addresses, and recipient email addresses. Mail logs, if available, may be obtained with a court order under 18 U.S.C. §2703(d), or a court order with an equivalent legal standard, or a search warrant. iCloud mail logs are retained up to 25 days.

c. Email Content and Other iCloud Content

For users that have enabled Advanced Data Protection, iCloud stores content for email, contacts, and calendars that the customer has elected to maintain in the account while the customer's account remains active. This data may be provided, as it exists in the customer's account, in response to a search warrant issued upon a showing of probable cause, or customer consent. This limited data is stored by Apple and additionally encrypted at the location of the server. For data Apple can decrypt, Apple retains the encryption keys in its U.S. data centers. Apple does not receive or retain encryption keys for customer's end-to-end encrypted data.

Advanced Data Protection uses end-to-end encryption, and Apple cannot decrypt certain iCloud content, including Photos, iCloud Drive, Backup, Notes, and Safari Bookmarks. In some circumstances, Apple may retain limited information related to these iCloud services that may be obtained, if available, with a court order under 18 U.S.C. §2703(d), or a court order with an equivalent legal standard, or a search warrant.

III. **iCloud Private Relay**

iCloud Private Relay is an internet privacy service offered as part of an iCloud+ subscription. Private Relay protects users' web browsing in Safari, DNS (Domain Name Space) resolution queries, and unencrypted http app traffic. Users must have an iCloud+ subscription and device with iOS 15, iPadOS 15, or macOS Monterey (macOS 12) or later to utilize iCloud Private Relay. More information about Private Relay can be found at https://support.apple.com/en-in/HT212614 and https://www.apple.com/privacy/docs/iCloud_Private_Relay_Overview_Dec2021.PDF.

When Private Relay is enabled, user web browsing requests are sent through two separate, secure internet relays. User IP address is visible to user network provider and to the first relay, which is operated by Apple. User DNS records are encrypted, so neither party can see the address of the website the user is trying to visit. The second relay, which is operated by a third-party content provider, generates a temporary IP address, decrypts the name of the website user requested and connects user to the site. Private Relay validates that the client connecting is an iPhone, iPad, or Mac. Private Relay replaces the user's original IP address with one assigned from the range of IP addresses used by the service. The assigned relay IP address may be shared among more than one Private Relay user in the same area.

Where user web browsing requests utilize Private Relay, Apple is not able to determine the user client IP address or the corresponding user account from the Private Relay IP addresses. Apple has no information to provide regarding the AppleID associated with the Private Relay IP address.

Note: iCloud Private Relay is not available in all countries or regions. If users have Private Relay enabled and travel somewhere Private Relay isn't available, it will automatically turn off and will turn on again when users re-enter a country or region that supports it.

M. Find My

Find My is a user-enabled feature by which an iCloud customer is able to locate his/her lost or misplaced iPhone, iPad, iPod touch, Apple Watch, AirPods, Mac, AirTag and/or take certain actions, including putting the device in lost mode, or locking or wiping the device. More information about this service can be found at https://www.apple.com/icloud/find-my/.

For the Find My feature to work for a customer who has lost their device, it must have already been enabled on that specific device before it was lost. The Find My feature on a device cannot be activated remotely, or after the device has been lost, or upon a request from a government or law enforcement agency. Device location services information is stored on each individual device and Apple cannot retrieve this information from any specific device. Location services information for a device located through the Find My feature is customer facing and Apple does not have content of maps or alerts transmitted through the service. The following support link provides information and steps that can be taken by a customer if an iOS device is lost or stolen: http://support.apple.com/en-us/HT201472.

Find My connection logs are available for a period up to 25 days; and, if available, may be obtained with a subpoena or greater legal process. Find My transactional activity for requests to remotely lock or erase a device, if available, may be obtained with an order under 18 U.S.C. §2703(d), or a court order with the equivalent legal standard, or a search warrant.

N. AirTag and Find My Network Accessory Program

The Find My app on iPhone, iPad, iPod touch, and Mac makes it easy for customers to locate personal items by attaching an AirTag or by using a product that is part of the Find My network accessory program.

With AirTag and iOS 14.5 and macOS 11.3 or later, customers may be assisted in finding missing personal items (keys, backpacks, luggage, etc.) using the Find My app. AirTag must be within Bluetooth range of the paired iPhone, iPad, or iPod touch in order to play a sound, or to use Precision Finding with compatible iPhone models. When not near its owner, the approximate location of AirTag may be provided if the AirTag is within range of a device in the Find My network, which is made up of hundreds of millions of Apple devices around the world. More information can be found at: https://support.apple.com/en-us/HT212227 and https://support.apple.com/en-us/HT210967.

The Find My network accessory program opens up the Find My network to third-party device manufacturer products (bikes, headphones, etc.) to utilize the service so customers can locate their supported third-party products with the Find My app with iOS 14.3 and macOS 11.1 or later.

To add AirTag or supported third-party products to the Items tab in the Find My app, customers must have an Apple ID, be signed into their iCloud account with Find My enabled, and register their AirTag or supported third-party products to their Apple ID. The interaction is end-to-end encrypted, and Apple cannot view the location of any AirTag or supported third-party products. More information can be found at https://support.apple.com/en-us/HT211331.

AirTag and Third-Party items that work with Apple's Find My app allow the paired account to share location visibility with up to five other accounts. Apple does not retain contact information for the accounts sharing AirTag and/or Third-Party item location and would only be able to return information for the item owner. All paired devices must be running iOS 17 or later for the AirTag sharing feature to work. More information can be found at: https://support.apple.com/guide/iphone/share-airtag-item-find-iphone-iph419cc5f28/ios

With a serial number, Apple may be able to provide the paired account details in response to a subpoena or greater legal process. AirTag pairing history is available for a period up to 25 days. The following support link provides information on finding an AirTag serial number: https://support.apple.com/en-us/HT211658. Information on a customer account associated with an AirTag may be available for a longer period of time where NFC tap activity has occurred. More information related to NFC capability can be found at the section "Get information about or disable an AirTag, Find My network accessory, or set of AirPods" in https://support.apple.com/en-us/HT212227.

Please note, expected AirTag serial number configuration is 12 characters, numbers, and letters, ending in "P0GV". (The character between the P and G is a zero). It should also be noted the maximum serial number length for third-party items that work with Apple's Find My app is 16 characters. Requests for serial numbers with either the letter "O" or "I" will yield no results. In instances where a legal request contains 5 or more serial numbers, Apple requests these serial numbers to also be submitted in editable electronic format (example Numbers, Excel, Pages or Word document).

O. Extracting Data from Passcode Locked iOS Devices

For all devices running iOS 8.0 and later versions, Apple is unable to perform an iOS device data extraction as the data typically sought by law enforcement is encrypted, and Apple does not possess the encryption key. All iPhone 6 and later device models are manufactured running iOS 8.0 or a later version of iOS.

For devices running iOS 4 through iOS 7, Apple may, depending on the status of the device, perform iOS data extractions, pursuant to California's Electronic Communications Privacy Act (CalECPA, California Penal Code sections 1546-1546.4). In order for Apple to perform an iOS data extraction for a device that meets these criteria, law enforcement should obtain a search warrant issued upon a showing of probable cause under CalECPA. Apart from CalECPA, Apple has not identified any established legal authority which requires Apple to extract data as a third-party in a law enforcement investigation.

P. IP Address Request

Requesting Apple customer data based on an IP address is often overly broad and imprecise. Before submitting legal process with an IP address as an identifier, Apple requests that law enforcement determine that the subject IP address is not a public or router IP address and not using Carrier-grade Network Address Translation (CGNAT) and confirm to Apple during service of the legal process that it

is a non-public IP address. Moreover, such requests must include a date restriction of no more than three days. In response to such a request, Apple may be able to produce connection logs (see below, section III.S) from which law enforcement can attempt to identify a particular Apple account/Apple ID to use as an identifier in a follow up legal process request. Apple customer data based on an IP address may be obtained with an order under 18 U.S.C. 2703(d) or court order meeting the equivalent legal standard or search warrant.

Q. Other Available Device Information

MAC Address: A Media Access Control address (MAC address), is a unique identifier assigned to network interfaces for communications on the physical network segment. Any Apple product with network interfaces will have one or more MAC addresses, such as Bluetooth, Ethernet, Wi-Fi, or FireWire. By providing Apple with a serial number (or in the case of an iOS device, IMEI, MEID, or UDID), responsive MAC address information, if available, may be obtained with a subpoena or greater legal process.

R. Requests for Apple Store CCTV Data

CCTV data may vary by store location. CCTV data is typically maintained at an Apple store for a maximum of 30 days. After this timeframe has passed, data may not be available. Requests which are solely for CCTV data can be sent to retailsecurity@apple.com. Government or law enforcement should provide store location, specific date, time, and related transaction information regarding the data requested.

S. Game Center

Game Center is Apple's social gaming network. Information regarding Game Center connections for a customer or a device may be available. Connection logs, if available, may be obtained with a subpoena or greater legal process. Game Center records of the specific games accessed, if available, may be obtained with an order under 18 U.S.C. §2703(d), or a court order with the equivalent legal standard, or a search warrant.

T. iOS Device Activation

When a customer activates an iOS device with a cellular service provider or upgrades the software, certain information is provided to Apple from the service provider or from the device, depending on the event. IP addresses of the event, ICCID numbers, and other device identifiers may be available. IP address information may be limited to the most recent 18 months. This information, if available, may be obtained with a subpoena or greater legal process.

Dual SIM: For devices featuring Dual SIM, carrier information for the nano SIM and/or eSIM, if available, may be obtained with a subpoena or greater legal process. An eSIM is a digital SIM that allows customers to activate a cellular plan from a carrier without having to use a physical nano-SIM. More information can be found at http://support.apple.com/en-us/HT209044.

U. Connection Logs

Connection activity for a customer or a device to Apple services such as Apple Music, Apple TV app, Apple Podcasts, Apple Books, iCloud, My Apple ID, and Apple Discussions, when available, may be obtained from Apple. These connection logs with IP addresses, if available, may be obtained with a subpoena or greater legal process. Transactional records, if available, may be obtained with an order under 18 U.S.C. §2703(d), or court order with the equivalent legal standard, or search warrant.

V. My Apple ID and iForgot Logs

My Apple ID and iForgot logs for a customer may be obtained from Apple. My Apple ID and iForgot logs may include information regarding password reset actions. Connection logs with IP addresses, if available, may be obtained with a subpoena or greater legal process. Transactional records, if available, may be obtained with an order under 18 U.S.C. §2703(d), or court order with the equivalent legal standard, or search warrant.

W. FaceTime

FaceTime communications are end-to-end encrypted and Apple has no way to decrypt FaceTime data when it is in transit between devices. Apple cannot intercept FaceTime communications. Apple has FaceTime call invitation logs when a FaceTime call invitation is initiated. These logs do not indicate that any communication between customers actually took place. Where only a phone number is provided, only currently registered FaceTime, iMessage, or security verified phone numbers may be produced. FaceTime call invitation logs are retained up to 25 days. FaceTime call invitation logs, if available, may be obtained with an order under 18 U.S.C. §2703(d), or court order with the equivalent legal standard, or search warrant.

X. iMessage

iMessage communications are end-to-end encrypted and Apple has no way to decrypt iMessage data when it is in transit between devices. Apple cannot intercept iMessage communications and Apple does not have iMessage communication logs. Apple does have iMessage capability query logs. These logs indicate that a query has been initiated by a device application (which can be Messages, Contacts, Phone, or other device application) and routed to Apple's servers for a lookup handle (which can be a phone number, email address, or Apple ID) to determine whether that lookup handle is "iMessage capable." iMessage capability query logs do not indicate that any communication between customers actually took place. Apple cannot determine whether any actual iMessage communication took place on the basis of the iMessage capability query logs. Apple also cannot identify the actual application that initiated the query. iMessage capability query logs do not confirm that an iMessage event was actually attempted. Where only a phone number is provided, only currently registered FaceTime, iMessage, or security verified phone numbers may be produced. iMessage capability query logs are retained up to 25 days. iMessage capability query logs, if available, may be obtained with an order under 18 U.S.C. §2703(d), or court order with the equivalent legal standard, or search warrant.

Y. Apple TV app

The Apple TV app allows customers to browse, purchase, subscribe to, and play TV shows and movies from Apple TV+, Apple TV Channels, and third party apps and services. Purchase and download history, may be available.

Requests for Apple TV app customer data must include the Apple device identifier (serial number, IMEI, MEID, or GUID) or relevant Apple ID/account email address. If the Apple ID/account email address are unknown, it is necessary to provide Apple with customer information in the form of full name **and** phone number, and/or full name **and** physical address in order to identify the subject customer account. Government or law enforcement officers may also provide a valid Apple order number or a complete credit/debit card number associated with an Apple TV app purchase(s). A customer name in combination with these parameters may also be provided, but customer name alone is insufficient to obtain information.

Please note: For data security purposes, when the legal process contains full credit, debit, DPAN or Apple gift card numbers, the complete legal process, including attachments, should be transmitted in a password-protected uneditable PDF and the password transmitted in a separate email. When legal process contains 5 or more search parameters, please include the search parameters in a password-protected editable document such as Numbers, Excel, Pages or Word. Apple will not download legal process documents through any links provided in an email due to system security standards. Additionally, providing a link to download the legal process will not be considered valid service of process.

Z. Sign in with Apple

Sign in with Apple is a more private way for customers to sign into third-party apps and websites with the customer's existing Apple ID. A Sign in with Apple button on a participating app or website allows a customers to set up an account and sign in with their Apple ID. Instead of using a social media account, or completing forms and selecting another new password, a customer can merely tap the Sign in with Apple button, review their information, and sign in quickly and securely with Face ID, Touch ID, or their device passcode. More information can be found at https://support.apple.com/en-us/HT210318.

Hide My Email is a feature of Sign in with Apple. It uses Apple's private email relay service to create and share a unique, random email address that forwards emails to a customer's personal email address. Basic customer information can be obtained with a subpoena or greater legal process.

AA. Apple Push Notification Service (APNs)

When users allow an application they have installed to receive push notifications, an Apple Push Notification Service (APNs) token is generated and registered to that developer and device. Some apps may have multiple APNs tokens for one account on one device to differentiate between messages and multi-media.

The Apple ID associated with a registered APNs token and associated records may be obtained with an order under 18 U.S.C. §2703(d) or a search warrant.

IV. Frequently Asked Questions

Q: Can I email Apple with questions regarding my legal process?
A: Yes, questions or inquiries regarding government legal process can be emailed to lawenforcement@apple.com.

Q: I need to personally serve Apple, where should I go?
A: All personal service can be made at Apple's Cupertino, California headquarters located at the following address:

Apple Inc.
20705 Valley Green Drive
Cupertino, CA 95014

Q: Can I serve a deposition subpoena directly on an Apple store?
A: No, all subpoenas for testimony, including subpoenas for deposition or trial testimony, need to be personally served on Apple as specified above.

Q: Does a device have to be registered with Apple in order to function or be used?
A: No, a device does not have to be registered with Apple in order for it to function or be used.

Q: Can Apple provide me with the passcode of an iOS device that is currently locked?
A: No, Apple does not have access to a customer's passcode.

Q: Can you help me return a lost or stolen device to the person who lost it?
A: In these cases, contact lawenforcement@apple.com. Please include the device serial number (or IMEI, if applicable) in your email and any additional relevant information. Information on finding the serial number is available here: https://support.apple.com/en-us/HT204308.

If customer information is available, Apple will contact the customer and provide details to contact law enforcement to recover the device. However, if the customer cannot be determined from available information, you may be instructed to submit a subpoena or other valid legal request.

Q: Does Apple keep a list of lost or stolen devices?
A: No, Apple does not keep a list of lost or stolen devices.

Q: What should be done with the produced files and records when law enforcement has concluded the investigation/criminal case?
A: Information and data provided to government or law enforcement containing personally identifiable information (including any copies made) should be destroyed after the related investigation, criminal case, and all appeals have been fully exhausted.

Q: Do you notify customers of legal process?
A: Yes, Apple's notice policy applies to account requests from law enforcement, government and private parties. Apple will notify customers and account holders unless there is a non-disclosure order or applicable law prohibiting notice, or where Apple, in its sole discretion, reasonably believes that such notice may pose immediate risk of serious injury or death to a member of the public, the case relates to a child endangerment matter, or where notice is not applicable to the underlying facts of the case.

Q: Can Apple intercept customers' communications pursuant to a Wiretap Order?
A: Apple can intercept customers' email communications, upon receipt of a valid Wiretap Order. Apple cannot intercept customers' iMessage or FaceTime communications as these communications are end-to-end encrypted.

Q: I am looking into whether a customer's email reach the requirements for interstate commerce. Where are the iCloud email servers located?
A: Apple's U.S. email servers are located in Arizona, California, Nevada, North Carolina, and Oregon.

Q: I requested information in the body of my email, why was it not provided?
A: Requests for information not included within the body of the signed subpoena, search warrant, or court order will be disregarded; Apple will only provide information that is specified in the actual executed legal process document.

Published June 2024