Lookout, Inc.
Personal Application Privacy Notice

Effective Date: 1/1/2020
Origination Date: 11/15/2016
Revision Date: 1/1/2023

1. Introduction

This document is our Personal Application Privacy Notice (the "Notice"), which describes what information we collect from you when you use the Lookout Personal Application (the "Personal App") and how we use that information. It is important that you read the Notice along with the Lookout Terms of Service (available at www.lookout.com/legal/terms) because both apply to your use of the Personal App. Any information that is collected from you by Lookout other than through the use of the Personal App will be subject to a different privacy notice.

This Notice may be revised to keep pace with changes in our products and services and laws applicable to Lookout and you. If we make material changes to this Notice, then we will notify you. If you do not wish your information to be subject to the revised Notice, you will need to close your account.

This Notice can be accessed from the Lookout mobile application login screen, from the settings in the Lookout Personal App, and from our company's website.

2. Information We Collect.

Lookout offers multiple tiers within the Personal App. Each tier offers increased access to Lookout security features. Information required to provide these services may vary and are listed in this document to help you understand what information we collect directly from you, from your device and how we use this information. Details regarding product features for the Personal App for iOS and Android devices can be found here https://www.lookout.com/products/personal/ios and https://www.lookout.com/products/personal/android.

a. Categories of Information. Lookout, or Lookout's partners, may collect the following categories of information from you in the course of using the Personal App:

i. ***Registration Data,*** including an email address and password.

ii. ***Device Data,*** such as equipment identifier (e.g., mobile phone number, device type and manufacturer, operating system type and version, wireless carrier/operator, network type, country of origin, Wi-Fi network SSID, Internet Protocol ("IP") address, and the dates and times of your requests.

iii. ***Application Data***, including metadata of all applications installed on your mobile device (including, but not limited to, the names of the apps and the versions of the apps), and in certain circumstances, we may also collect a copy of part or entire copies of application files on your device if we encounter an application that we have not previously analyzed. This data is pseudonymized and is maintained in aggregate to ensure an individual cannot be identified from other customers. We may also collect information about how applications behave on your device (e.g., whether an application is sending premium-rate text messages that may charge money to your phone bill) and the network services with which your applications communicate.

iv. ***Location Data.*** Some features we offer work better if we can locate your mobile device. With your consent, which is provided during initial registration, Lookout may collect location information in two ways. We may receive it directly from your mobile device, or, in some situations, we may infer location data from cell tower or Wi-Fi hotspot information. We may use third-party service providers to translate that information into usable location information. To prevent location data from being shared go to your mobile device settings and turn off location services, but doing so may affect the features that Lookout can provide.

v. ***Theft Alerts Data,*** including Location Data and a picture that is taken when the Theft Alerts feature is activated.

vi. ***Payment Data,*** including your credit card number, expiration date, security code and other applicable billing information, may be collected directly by Lookout's partners if you have purchased the Premium and Premium Plus versions of the application.

vii. ***Web Content Data,*** including URLs and domains for malicious content and content that needs additional analysis to determine if those URLs are unsafe (e.g., if the URLs contain phishing attacks or malware). Lookout does not collect browsing history.

viii. ***Identity Theft Protection Data***, which you have the option to provide if you purchased Lookout Premium Plus, including private information (such as a driver's license number, social security number, passport number, or other identification number), financial information (such as a bank account, debit and credit card numbers), medical insurance number, and other data about you, including name and title (or other people you enroll in the service), may be collected directly by Lookout's partner, CSIdentity (now part of Experian).

ix. ***Analytics Data,*** including third party tools such as Mixpanel, Braze, and mParticle to help us analyze and aggregate data regarding your use of our Services. We encourage you to read the MixPanel Privacy Policy, Braze Privacy Policy, and mParticle Privacy Policy.

Given that product features will vary by tier, Lookout may collect different types of information based on the tier you are using as described further below.

b. Information Lookout Collects for the Lookout Basic Personal App

i. ***Registration Data.*** To create an account, you must provide an email address and a password.

ii. ***Device Data.*** When you use Lookout Services, our servers record certain information about your mobile device as described in Section 2(a)(ii) above.

iii. ***Application Data.*** When you use Lookout Services, we collect application files and download a copy of part or entire copies of application files on your device if we encounter an application that we have not previously analyzed as described in Section 2(a)(iii) above. For clarity, Lookout does not collect user data you enter into those applications. Because Lookout does not collect any user data you enter into the applications on your mobile device, Lookout does not collect, read, review, or scan your emails, or text messages. Lookout does not collect your photos, or videos, but may scan such files locally on the device to protect you from certain threats that hide inside photo or video files.

iv. ***Location Data.*** If activated, Lookout's Missing Device feature, including the ability to Locate and Scream your device remotely, uses Location Data to help you locate your phone near its last known location if you lose it and its battery dies. Additionally, if you have Signal Flare enabled, this feature collects Location Data and sends it back to Lookout when your battery is running low.

c. Information Lookout Collects for the Lookout Premium Personal App

Lookout collects the same information stated in the Lookout Basic Personal App, but in addition to this information, Lookout's partner will also collect Payment Data directly from you to allow you to access premium features, Web Content Data to use the Safe Browsing feature, and Theft Alerts Data to provide the Theft Alerts feature as described below.

i. ***Payment Data.*** If you purchase a Premium or Premium Plus Lookout Service subscription directly from us, we use a third-party payment processor to collect Payment Data. Our third-party vendor will use this information to bill you for services. Lookout will have information regarding your Premium and/or Premium Plus account. This information will include the amount you paid, and the method of payment. We will not have your credit card or bank information; this information remains with the third-party payment processor. If you purchase the Lookout App from an App Store or through your Carrier plan your payment information will be managed by that App Store or Carrier. Payment does not go to Lookout. Your payment could be processed in various ways. In order to provide our services to you, the App Store will send Lookout confirmation of your purchase. Carriers may share your phone number, subscriber ID, SKU and other non-financial information. The App Store and your Carrier will not share credit card or billing data. For additional information, please refer to your App Store or Carrier's payment processing policies and procedures.

ii. ***Web Content Data.*** To provide the Safe Browsing service, Lookout uses Web Content Data. If you do not want us to record the unsafe URLs you visit, you may turn Safe Browsing off; all other Lookout features will continue to function.

iii. ***Theft Alerts Data.*** When Theft Alerts is activated a photo is taken. The picture and Location Data (GPS location) are stored briefly on our servers so we can send you an email with the picture and a map of your device's

location. The picture is then deleted from our server. We send the email to the address associated with your account so remember to keep your email address up to date in your account settings.

d. Information Lookout Collects for the Lookout Premium Plus Personal App

Lookout collects the same information stated in the Premium Personal App, but in addition to this information, Lookout's partner will also collect Identity Theft Protection Data from you.

i. ***Identity Theft Protection Data.*** When you use the Identity Theft Protection feature you may input the Identity Theft Protection Data described above for the purposes of enrolling in certain identity protection monitoring services provided by our third-party partner, CSIdentity (now part of Experian). The information that CSIdentity collects and stores about you will depend on the information you have inputted within the Personal App. CSIdentity may need to communicate your Identity Theft Protection Data to third party service providers (such as identification verification companies, consumer reporting agencies, credit bureaus, payment validation companies, law enforcement agencies, and others) in order to provide those services to you.

e. Information Lookout collects from Third Party Sources

Lookout receives Analytics Data from third parties as described above.

3. How We Use Your Information.

When we collect your information, we store it and associate it with your account unless otherwise noted. Please note that we need certain types of information so that we can provide the services to you. If you do not provide us with such information, or ask us to delete it, you may no longer be able to access the services. We take your privacy very seriously and will only use and disclose this information for the business and commercial purposes described in this Notice. How we use your information will vary depending on the type of data as described below:

a. Application Data. We use this data to provide our services by conducting scans of application files to determine if any applications are behaving maliciously. We also pseudonymize data and aggregate the information to produce popularity of applications by region, and to perform our mobile threat analysis. This mobile threat analysis data will remain pseudonymized to ensure data privacy. Combining customer data in a secure and confidential way helps Lookout to better understand current security threats, and to improve the Lookout services.

b. Device Data. Automatic scans of your device may occur periodically to collect details about the applications, devices and operating system files on your device. Lookout will gather the results of scans performed by our services and the most current security disposition of the device. In addition, regular updates of threat definitions will be performed. These activities help to protect your mobile end point by allowing the Personal App to detect and address threats on your mobile device. Where available, Lookout may use client device information to let you know you need to update your operating system. In addition to using the information you provide to us and the information we collect from your mobile endpoint device to deliver Lookout services, we also use the information collected from your device to perform data analytics. These analytics provide important information which helps to improve the features and usability of our products. We analyze information such as how often you use the Lookout application on your mobile endpoint device, the events that occur within the Lookout application on your mobile endpoint device and where the Lookout application was downloaded onto your mobile endpoint device. We also use this information in aggregate to perform analysis on known and new mobile threats.

c. Identity Theft Protection Data. CSIdentity will use this information to verify your identity and provide you with the requested Identity Protection services. If you upgrade to a Premium Plus subscription that includes identity theft insurance, our partners will use your information to provide you with assistance and applicable insurance coverage if your identity is compromised.

d. Location Data. Lookout's Missing Device feature includes the ability to Locate and Scream your device remotely from your Personal account at lookout.com, and Lookout uses Location Data to help you locate your phone near its last known location if you lose it and its battery dies. If you have enabled Signal Flare, it collects location information and sends it back to Lookout when your battery is running low. We save the phone's location to

lookout.com at the time we receive the low battery alert. This feature can be turned on or off via the Personal App settings.

e. **Registration Data**. We may use your email address to send you information about product announcements and special promotions from Lookout or our business partners. If you email Lookout for support, we may retain that information in order to provide you with support and to improve our services. We may use your email address to communicate with your device about the services, including sending privacy or security related notices and notifying you of major Lookout services changes.

f. **Theft Alerts Data**. We use this information to perform the theft alert services.

g. **Web Content Data**. Safe Browsing is a feature designed to identify and warn you of unsafe URLs so that you can choose to avoid loading them. URLs visited are pseudonymized and sent to Lookout to perform security scans. We use the record of unsafe URLs you visit to provide you with notice that the URL you attempted to reach is unsafe.

4. How We Disclose Your Information

This section describes how Lookout may share and disclose your information.

a. **Third Party Service Providers and Partners**. We may share your information with third party service providers of products and services integrated with our software that need to know your information to fulfill your product or service requests, support our products and services, analyze data for product performance, and product improvement purposes. For example:

   i. When using the Identity Theft Protection service, your information is collected by our partner, CSIdentity (now part of Experian) to provide the service to you. CSIdentity may in turn provide your data to third parties such as identification verification companies, consumer reporting agencies, credit bureaus, payment validation companies, law enforcement agencies, and others for purposes of providing you with the services requested. CSIdentity may also provide you with monitoring and alerts and obtain information and reports about you (or about others that you have enrolled) in order to provide the Identity Protection Services, including address history, name, alias and other reports. We require that CSIdentity and its service providers use data collected from you only for purposes of providing services through the Lookout App Premium Plus Product.

   ii. We may share your information with our resellers or other mobile operators to ensure proper delivery of your purchase and related support services and perform business-related functions.

   iii. We may use your information to conduct market research and engage in joint promotional activities with companies that have products that can add value to Lookout products or services (for example, with mobile operators).

b. **Third Party Payment Partners**. We may allow services providers to collect information directly from you to perform accounting, auditing, billing reconciliation, and collection activities.

c. **To Comply with Law**. We may disclose your information consistent with the law to, for example: (i) comply with a law, regulation, or legal process (including to meet national security or law enforcement requirements); (ii) protect the safety or security of any person, entity or facility; (iii) address potential violations of our Notice; (iv) investigate fraud, security, or technical issues; or (v) protect Lookout's or a third party's rights or property, our employees, users and the public. We strongly believe that you have a right to know if we are required by law to disclose your information. As such, before we disclose your information in response to a law enforcement request (for example, a subpoena or court order), we will notify you at the email listed in your account, unless (a) we are prohibited from doing so or (b) in emergency cases where notice could create a risk of injury or death, or the case involves potential harm to minors. Furthermore, nothing in this Notice is meant to limit any legal defenses or objections that you may have to a third party, including the government's, request to disclose your information.

d. **During a Change to Lookout's Business**. We may also disclose your information to an actual or potential buyer (and its agents and advisers) in connection with any actual or proposed purchase, merger, or acquisition of any

part of our business, provided that we inform the buyer it must use your information only for the purposes disclosed in this Notice.

e. **Pseudonymized and Aggregated Data**. For data analysis we pseudonymize, aggregate and summarize data that may include some of your data. We may share reports resulting from this data analysis publicly, in order to help others understand mobile threats and gain insights into particular mobile application behavior.

f. **With Consent**. We may also disclose your information to third parties when we have your consent to do so.

5. Your Choices

a. You Can Access and Update Your Settings

You may update the settings of your Lookout account via the 'Settings' page on our mobile application, or by logging in via our website at https://my.lookout.com/user/login, to modify certain settings that affect what data is shared with us. To protect your privacy and security, we require your username and password in order to verify your identity before granting you access or making changes to your account.

b. Email Opt-Outs

You may opt out of receiving promotional communications from Lookout by using the unsubscribe link within each email. Although opt-out requests are usually processed immediately, please allow ten (10) business days for a removal request to be processed. Even after you opt out from receiving promotional messages from us, you will continue to receive transactional and product-related messages from us regarding Lookout Services. You can opt-out of some of these notification messages in your account settings.

6. Data Retention

Lookout will retain your information, including your Personal Data (as that term is defined by the GDPR), only as long as reasonably necessary to provide our products and services to you or as otherwise required for legal compliance purposes.

7. Security

a. Lookout's Responsibilities.

Lookout is a security company, and securing your data is important to us. Lookout uses commercially reasonable physical, managerial, and technical safeguards to ensure appropriate technical and organizational measures appropriate to the risk of processing your information. For example, we use a combination of firewalls, authentication, physical security, and other safeguards to protect your account and your data. When you enter sensitive information (such as Location Data) within the Lookout app we encrypt that information while in transit and at rest using secure socket layer technology (SSL). We also perform third-party penetration tests to harden our systems from attack. Lookout takes every reasonable effort to implement controls to protect against complex technological threats and other criminal threats, as well as to guard against negligent employees.

Because no method of transmission over the Internet or method of electronic storage is 100% secure, we cannot ensure or warrant the security of any information, data or content that Lookout receives on your behalf to operate the Lookout services, or that you transmit to Lookout. All such receipt or transmission of your information is provided under your own free will and at your own risk. We cannot guarantee that such information will not be accessed, disclosed, altered, or destroyed by breach of any of our physical, technical, or managerial safeguards

If Lookout learns of a security breach that may affect you, we will attempt to notify you electronically so that you can take appropriate protective steps. Lookout will also post a notice on the Lookout services if a security breach occurs. Depending on where you live, you may have a legal right to receive notice of a security breach in writing.

b. Your Responsibilities.

You are responsible for maintaining the secrecy of your password at all times. We recommend a strong password that you do not use with other services. If you believe your password has been compromised, please change your

password immediately via the Lookout website, or contact us at support@lookout.com for assistance. You are responsible for ensuring that the email address associated with your account is accurate. We use that email to contact you about service updates, changes to our policies, and account activities such as requests for your information or locate attempts on your device. Lookout is not responsible for information transmitted to a third party as a result of a user's providing an incorrect email address.

8. Users Under 16

Lookout does not knowingly collect or store any Personal Data about children under the age of 16 unless they are part of a Multiple Device Plan purchased by a parent who consents to such collection and storage as described in the Lookout Terms of Service. If you believe a child is using this service without parental consent, please contact us at privacy@lookout.com.

9. International Data Transfers

Lookout is a San Francisco-based company with servers housed in the United States. Personal Data collected from users outside the United States is transferred to the United States. If you are using the Lookout Services from outside the United States your information may be transferred to, stored, and processed in the United States where our servers are located and our databases are operated.

10. Additional Terms for California Residents

a. Personal Information.

In accordance with the California Consumer Privacy Act ("CCPA"), as amended by the California Privacy Rights Act, below is a list of the categories of Personal Information (as that term is defined by the CCPA) that we collect (whether through the Personal App or elsewhere), the categories of sources we collect them from, the commercial purpose for which the information was collected, and the categories of third parties with which we share the Personal Information. The information listed in the chart below is accurate of the preceding 12 months.

Categories of Personal Information	Categories of Sources	Commercial Purpose	Categories of entities that we sell, share, or disclose Personal Information to for a Business Purpose
Identifiers, including email address, IP address, Wifi SSID and other device identifiers	Consumer	Provide Service, Improve Service, Customer Service, Analytics	Data analytics providers, service providers, and contractors
*Identity Theft Protection Identifiers, including SSN, driver's license number, credit card and bank account numbers	Consumer	Provide Service	Service providers, and contractors
Geolocation data	Consumer	Provide Service	Service providers, and contractors
Information regarding a consumer's interaction with websites or applications	Consumer	Provide Service	Service providers, and contractors

*All Identity Theft Protection identifiers are inputted directly by the Consumer, are stored by Lookout's third party service provider, CSID (now part of Experian), and used solely for the purposes of providing the services.

b. Your Rights.

In accordance with the CCPA, and subject to exceptions, California Consumers (as that term is defined in the CCPA) have the following rights:

i. **Access.** You have the right to request that Lookout disclose and deliver the categories of Personal Information Lookout has collected about you, or the specific pieces of Personal Information the business has collected about you;

ii. **Deletion.** You have the right to request the deletion of your Personal Information in certain situations, subject to certain exceptions outlined in the law;

iii. **Correction.** You have the right to correct or amend the Personal Information we have on file about you;

iv. **Non-Discrimination.** You have the right to not be discriminated against, including but not limited to the right not to be charged a different price for the services or denying you access to the services, on the basis of your decision to exercise any of your rights in this Section. We will not discriminate against you for exercising any of your rights under the CCPA.

v. **Opt-Out.** Lookout does not sell or share any Personal Information of its users of the Personal App, so this right is not applicable to you.

vi. **Limit Use of Sensitive Personal Information.** Lookout does not process your "Sensitive Personal Information" (as that term is defined under the CCPA) for any purposes beyond those permitted in Section 7027(m) of the CCPA regulations, so this right is not applicable to you.

You may exercise your rights to access your information or to delete your information through two methods: (1) complete the webform accessible through https://personal.support.lookout.com, or (2) send a request to Privacy@Lookout.com. As stated above in Section 5(a), to protect your privacy and security, we require you to verify your identity by logging into your account with your username and password before granting your request to access or delete your Personal Information. If we cannot verify your identity, then we shall not disclose any specific pieces of Personal Information in response to an access request, and we shall deny your request to delete Personal Information in response to a deletion request. For requests to delete your information, Lookout shall use a two-step process where you must first, clearly submit the request to delete and then second, separately confirm that you want your Personal Information deleted. As a California Consumer, you may have an authorized agent make an access or deletion request on your behalf, provided that the authorized agent has your written permission, and you are able to verify your own identity directly with Lookout.

11. Additional Terms for European Economic Area ("EEA") Residents

a. Legal Basis for Processing.

If you are a visitor from the EEA, Lookout is the data controller of your Personal Data (as that term is defined in the General Data Protection Regulation ("GDPR")). The legal basis for collecting and using your personal data as set out in this Notice will depend on the Personal Data concerned and the specific context in which we collect it. However, we will normally collect Personal Data from you only where: (a) use of your Personal Data is necessary to perform our obligations under any contract with you (for example, to comply with the Terms of Service which you accept by downloading and using our apps); or (b) use of your Personal Data is necessary for our legitimate interests or the legitimate interests of others (for example, to ensure the security of the Lookout Services, operate and market the Lookout Services, ensure safe environments for our personnel and others, make and receive payments, prevent fraud and to know the customer to whom we are providing the Lookout Services); or (c) we have your consent to do so (such as for some of our marketing activities). Some processing is done to comply with applicable law.

b. Privacy Shield

Lookout has self-certified with the E.U.-U.S. Privacy Shield and Swiss-U.S. Privacy Shield framework as set forth by the U.S. Department of Commerce regarding the collection, use, and retention of Personal Data from E.U. States, the United Kingdom and Switzerland. These frameworks were developed to enable companies to comply with data protection requirements when transferring personal data from the European Union, the United Kingdom and Switzerland to the United States. To learn more about the Privacy Shield, view a list of entities who have current certifications under Privacy Shield, please visit http://www.privacyshield.gov.

As required under the principles, when Lookout receives information under the Privacy Shield and then transfers it to a third-party service provider acting as an agent on Lookout's behalf, Lookout has certain liability under the Privacy Shield if both (i) the agent processes the information in a manner inconsistent with the Privacy Shield and (ii) Lookout is responsible for the event giving rise to the damage.

With respect to personal information received or transferred pursuant to the Privacy Shield Frameworks, we are subject to the regulatory enforcement powers of the U.S. Federal Trade Commission. In certain situations, we may be required to disclose personal information in response to lawful requests by public authorities, including to meet national security or law enforcement requirements.

If you are dissatisfied with the manner in which we have addressed your concerns about our privacy practices and we process your personal information in accordance with Privacy Shield, you may seek further assistance, at no cost to you, from our designated Privacy Shield independent recourse mechanism, which you can learn more about by visiting https://www.jamsadr.com/eu-us-privacy-shield. You also have a right to lodge a complaint with the relevant supervisory authority. However, we encourage you to contact us first, and then we will do our very best to resolve your concern. You may also select binding arbitration for unresolved complaints but prior to initiating such arbitration, you must: (1) contact Lookout and afford us the opportunity to resolve the issue; (2) seek assistance from Lookout's designated independent recourse mechanism above; and (3) contact the U.S. Department of Commerce (either directly or through a European Data Protection Authority) and afford the Department of Commerce time to attempt to resolve the issue. To find out more about the Privacy Shield's binding arbitration scheme please see https://www.privacyshield.gov/article?id=ANNEX-I-introduction. Each party shall be responsible for its own attorney's fees. Please be advised that, pursuant to the Privacy Shield, the arbitrator(s) may only impose individual-specific, non-monetary, equitable relief necessary to remedy any violation of the Privacy Shield Principles with respect to the individual. Lookout is subject to the investigatory and enforcement powers of the U.S. Federal Trade Commission (FTC).

Please note that Lookout is aware of the Court of Justice of the European Union (CJEU) invalidating Privacy Shield as a certification of EU privacy law compliance. Lookout has always maintained its obligations independently through privacy policies with partners, customers, and users of our website. Lookout commits to continue to meet the applicable requirements for protection of personal information as required under applicable law, regulation, and other governing authority. Lookout has further committed to cooperate with the panel established by the EU data protection authorities (DPAs) and the Swiss Federal Data Protection and Information Commissioner (FDPIC) with regard to unresolved Privacy Shield complaints concerning data transferred from the EU and Switzerland. Lookout will continue to monitor developments related to the EU-US Data Privacy Framework, and will ensure its treatment of personal information is consistent with applicable laws.

12. Data Subject Rights

If you are a resident of the United Kingdom, EEA, or another jurisdiction with an applicable data protection law (such as Virginia, Colorado, Connecticut, and Utah), you may have certain rights in relation to your Personal Data. These rights may be subject to certain exemptions. These rights may include:

i. **Access.** You may have the right to request a copy of the Personal Data that we are processing about you. If you require additional copies, we may need to charge a reasonable fee;

ii. **Rectification.** You may have the right to require the correction of any mistake in the Personal Data, whether incomplete or inaccurate, that we hold about you;

iii. **Deletion.** You may have the right to require the erasure of Personal Data concerning you in certain situations, such as where we no longer need it or if you withdraw your consent (where applicable). In addition to the rights granted under the section above entitled, "You Can Access and Update Your Privacy Settings," you may contact us at privacy@lookout.com with your request;

iv. **Portability.** You have the right to receive the Personal Data concerning you that you have provided to us, in a structured, commonly used, and machine-readable format and have the right to transmit that data to a third party in certain situations;

v. **Objection.** You may have the right to (i) object at any time to the processing of your Personal Data for direct marketing purposes and (ii) object to our processing of your Personal Data where the legal ground of such processing is necessary for legitimate interests pursued by us or by a third party.

vi. **Restriction.** You have the right to request that we restrict our processing of your Personal Data in certain circumstances, such as when you contest the accuracy of that personal information;

vii. **Withdrawal of consent.** If we rely on your consent for processing your Personal Data, you have the right to withdraw that consent at any time.

viii. **Lodge a complaint to a data supervisory authority.** Depending on your jurisdiction, you may have the right to lodge a complaint with your local data supervisory authority if you believe we are in violation of applicable data protection law.

If you wish to exercise any of these rights, please contact us at privacy@lookout.com. We will respond to your request in the time period required under applicable law. Please note that we may need to verify your identity prior to complying with your request. We will verify your identity by sending you an email to the email address associated with your account or by asking you to provide additional information associated with your account. You may also designate an authorized agent to submit a request on your behalf (though we may still need to verify your identity).

13. Contact Us if You Have Any Questions or Concerns

Please contact our Data Protection Officer at privacy@lookout.com, or by postal mail at Lookout, Inc., Attn: Michael Musi, Data Protection Officer, 3 Center Plaza, Suite 330, Boston, MA (USA) 02108, with any questions or comments about this Notice. Residents of the EEA may also contact by sending inquiries to the attention of Mr. Wim Van Campen, VP, Sales EMEA, Florapark 3, 2012 HK Haarlem, Netherlands.