

Complaint

IN THE MATTER OF

MICROSOFT CORPORATION

CONSENT ORDER, ETC., IN REGARD TO ALLEGED VIOLATIONS OF
SEC. 5 OF THE FEDERAL TRADE COMMISSION ACT

Docket C-4069; File No. 0123240

Complaint, December 20, 2002--Decision, December 20, 2002

This consent order addresses representations made – for Passport Single Sign-In service, an online authentication service, and for two add-on services that respectively provide online purchasing and parental consent services – by Respondent Microsoft Corporation. The order, among other things, prohibits the respondent from misrepresenting (1) what personal information is collected from or about consumers; (2) the extent to which the respondent's product or service will maintain, protect or enhance the privacy, confidentiality, or security of any personally identifiable information collected from or about consumers; (3) the steps the respondent will take with respect to personal information it has collected in the event that it changes the terms of the privacy policy in effect at the time the information was collected; (4) the extent to which the service allows parents to control what the information their children can provide to participating sites or the use of that information by such sites; and (5) any other matter regarding the collection, use, or disclosure of personally identifiable information. The order also requires the respondent to establish and maintain a comprehensive information security program in writing that is reasonably designed to protect the security, confidentiality, and integrity of personal information collected from or about consumers. In addition, the order requires the respondent to obtain within one year, and on a biannual basis thereafter, for twenty years, an assessment and report from a qualified, objective, independent third-party professional certifying that the respondent has in place a security program (1) that provides protections that meet or exceed the protections required by the order; and (2) is operating with sufficient effectiveness to provide reasonable assurance that the security, confidentiality, and integrity of consumers' personal information has been protected.

Participants

For the Commission: *Ellen Finn, Eric Imperial, Mamie Kresses, Jessica L. Rich, Louis Silversin, Gerard R. Butters and Paul A. Pautler.*

For the Respondent: *Charles E. Buffon, Covington & Burling, and Linda Norman, Microsoft.*

Complaint

COMPLAINT

The Federal Trade Commission, having reason to believe that Microsoft, a corporation (“respondent”) has violated the provisions of the Federal Trade Commission Act, and it appearing to the Commission that this proceeding is in the public interest, alleges:

1. Respondent Microsoft is a Washington corporation with its principal office or place of business at One Microsoft Way, Redmond, Washington 98052. Respondent, a software and technology company, has advertised and promoted its sign-on and online wallet services, Passport and Passport Express Purchase (aka Passport Wallet), through the company’s Web site at www.passport.com and elsewhere on the Internet.
2. The acts and practices of respondent as alleged in this complaint have been in or affecting commerce, as “commerce” is defined in Section 4 of the Federal Trade Commission Act.

Passport Security

3. Following the launch of Passport in October 1999, respondent disseminated or caused to be disseminated various versions of a “Microsoft .NET Passport Q&A” on Passport.com, including but not necessarily limited to that attached as Exhibit A, containing the following statements:

Security and Privacy**How secure is .NET Passport?**

.NET Passport achieves a high level of Web Security by using technologies and systems designed to prevent unauthorized access to your personal information.

Complaint

Exhibit A, Microsoft .NET Passport Q&A,
<http://www.passport.com/Consumer/ConsumerQA.asp?lc>.

4. Respondent also disseminated or caused to be disseminated on the home page of its Web site at Passport.com various advertisements, including but not necessarily limited to that shown in Exhibit B, containing the following statements:

Security

Use .NET Passport from any computer on the Internet.
Your .NET Passport is protected by powerful online security technology and a strict privacy policy.

Exhibit B, Passport Home Page,
<http://www.passport.com/Consumer/Default.asp?lc=1033>.

5. Respondent also disseminated or caused to be disseminated various privacy policies on Passport.com, including but not limited to the attached Exhibit C, containing the following statements:

**SECURITY OF YOUR PERSONAL
INFORMATION**

Your .NET Passport information is stored on secure .NET Passport servers that are protected in controlled facilities.

Exhibit C, Microsoft .NET Passport Privacy Policy,
<http://www.passport.com/Consumer/PrivacyPolicy.asp?lc=1033>.

6. Through the means described in Paragraphs 3-5, respondent represented, expressly or by implication, that it maintained a high level of online security by employing sufficient measures reasonable and appropriate under the circumstances to maintain and protect the privacy and confidentiality of personal information obtained from or about consumers in connection with the Passport and Passport Wallet services.

Complaint

7. In truth and in fact, respondent did not maintain a high level of online security by employing sufficient measures reasonable and appropriate under the circumstances to maintain and protect the privacy and confidentiality of personal information obtained from or about consumers in connection with the Passport and Passport Wallet services. In particular, respondent failed to implement and document procedures that were reasonable and appropriate to: (1) prevent possible unauthorized access to the Passport system; (2) detect possible unauthorized access to the Passport system; (3) monitor the Passport system for potential vulnerabilities; and (4) record and retain system information sufficient to perform security audits and investigations. In light of these deficiencies, taken together, the representation set forth in Paragraph 6 was false or misleading.

Passport Wallet Security

8. Respondent has promoted its Passport Express Purchase service, also referred to as Passport Wallet, as an online service that facilitates consumers' online purchases by transmitting credit card numbers, billing information, and shipping information stored in their Passport wallet to participating Express Purchase sites.

9. Following the launch of Passport Wallet in October 1999, respondent disseminated or caused to be disseminated on the home page of its Web site at Passport.com various advertisements, including but not necessarily limited to that shown in Exhibit B, containing the following statements:

Store information in .NET Passport wallet that will help you make faster safer online purchases at any .NET Passport express purchase site.

Exhibit B, Passport Home Page,
<http://www.passport.com/Consumer/Default.asp?lc=1033>.

Complaint

10. Respondent also disseminated or caused to be disseminated various versions of a “Microsoft .NET Passport Q&A” on Passport.com, including but not necessarily limited to that attached as Exhibit A, containing the following statements:

What is Microsoft .NET Passport and what can I do with it?

* * *

With a .NET Passport, you can:

* * *

Make faster, more secure online purchases with .NET Passport express purchase.

Exhibit A, Microsoft .NET Passport Q&A,
<http://www.passport.com/Consumer/ConsumerQA.asp?lc>.

11. Through the means described in paragraphs 9 and 10, respondent represented, expressly or by implication, that purchases made at a Passport Express Purchase site with Passport Wallet are safer or more secure than purchases made at the same Passport Express Purchase site without using the Passport Wallet.

12. In truth and in fact, purchases made at a Passport Express Purchase site with Passport Wallet are not, for most consumers, safer or more secure than purchases made at the same Passport Express Purchase site without using the Passport Wallet. Most consumers making credit card purchases at a Passport Express Purchase site receive identical security whether they use Passport Wallet to complete a transaction or purchase directly from the Passport Express Purchase site without using a Passport Wallet. Therefore, the representations set forth in paragraph 11 were false or misleading.

Complaint

Passport Privacy - Data Collection

13. Respondent has disseminated or caused to be disseminated various privacy policies on Passport.com, including but not limited to the attached Exhibit C, which contains the following statements:

This Privacy Statement discloses the privacy practices for the .NET Passport Web Site and .NET Passport Services in accordance with the requirements of the TRUSTe Privacy Program. When you visit a web site displaying the TRUSTe trademark, you can expect to be notified of [w]hat personally identifiable information of yours is collected. . . .

Exhibit C, Microsoft .NET Passport Privacy Policy,
<http://www.passport.com/Consumer/PrivacyPolicy.asp?lc=1033>.

14. This privacy statement also described in detail the information collected from or about consumers in connection with their use of the Passport, including, but not limited to: what information is collected by Passport when a consumer registers at the Passport.com site; what information is collected by Passport and by a participating site when a consumer registers for Passport through that participating site; what information is collected by participating sites when a consumer signs in with a Passport; “operational” information generated in connection with a Passport account; the association of a unique identification number with every Passport account; and the collection of sign-in and other information in temporary cookies that are deleted when the consumer signs out of Passport.

15. Through the means described in paragraphs 13-14, respondent represented, expressly or by implication, that Passport did not collect any personally identifiable information other than that described in its privacy policy.

Complaint

16. In truth and in fact, Passport did collect personally identifiable information other than that described in its privacy policy. In particular, Passport collected, and maintained for a limited period of time, a personally identifiable record of the sites to which a Passport user signed in, along with the dates and times of sign in, which customer service representatives linked to a user's name in order to respond to a user's request for service. Therefore, the representation set forth in paragraph 15 was false or misleading.

Kids Passport

17. Respondent has promoted its Kids Passport service as an online service that assists parents in protecting their children's online privacy.

18. Since the introduction of Kids Passport in April 2000, respondent has disseminated or caused to be disseminated various Kids Passport web pages and privacy policies, including but not necessarily limited to the attached Exhibits D and E, which contain the following statements:

A. **Welcome to Kids Passport**
Helping parents protect their children's privacy online

...

Learn about the Children's Online Privacy Protection Act

Discover how Passport Kids is helping parents to keep their children's identity safe online.

...

Microsoft Kids Passport is a free service that helps you conveniently protect and control your children's online privacy. . . With Kids Passport, you can grant or deny consent to participation (*sic*) web sites (including the Microsoft family of web

Complaint

sites) to collect personal information from your children. In addition, you can make specific choices for each child and for each site, all in one convenient, centralized location.

Exhibit D, Kids Passport web pages,
<http://kids.passport.com>.

B. Microsoft Kids Passport Privacy Statement

Microsoft is especially concerned about the safety and protection of children's personal information collected and used online. Microsoft Kids Passport ("Kids Passport") allows parents to consent to the collection, use and sharing of their children's information with Passport participating sites and services that have agreed to use Kids Passport as their parental consent process.

...

**USE OF CHILDREN'S PERSONAL
INFORMATION BY PASSPORT**

...

Passport does not share this information contained in your child's Passport profile with third parties, except for Passport participating sites where you have consented to such sharing, or as otherwise disclosed in this statement.

...

**CONTROL OF CHILDREN'S PERSONAL
INFORMATION**

Kids Passport allow you to limit the amount of information shared with the sites and services participating in the Kids Passport program. You can choose to allow Passport to share all of the information in your child's Passport profile with a

Complaint

participating site or service, or you can limit the information shared to just a unique identifier or age range.

...

Exhibit E, Microsoft Kids Passport Privacy Statement,
[http://www.passport.com/
consumer/privacy/policy.asp/PPIcid=1033](http://www.passport.com/consumer/privacy/policy.asp/PPIcid=1033).

19. Through the means described in Paragraph 18, respondent represented, expressly or by implication, that the Kids Passport service provided parents with control over the information their children could provide to participating Passport sites and the use of that information by such sites.

20. In truth and in fact, the Kids Passport service did not provide parents with control over the information their children could provide to participating Passport sites and the use of that information by such sites. For instance, once a parent set up a child's Passport account and provided consent for the collection and/or disclosure of the types of personal information listed in respondent's privacy policy, respondent permitted the child to edit or change certain fields of personal information and change account settings set by the parent. Respondent also failed to clearly inform parents that in some instances information would be disclosed to Passport Web sites that do not participate in the Kids Passport service. Therefore, the representations set forth in paragraph 19 were false or misleading.

21. The acts and practices of respondent as alleged in this complaint constituted unfair or deceptive acts or practices in or affecting commerce in violation of Section 5(a) of the Federal Trade Commission Act.

THEREFORE, the Federal Trade Commission this twentieth day of December, 2002, has issued this complaint against respondent.



Microsoft® .NET Passport Q&A

Click a topic below for answers to common questions about the Microsoft .NET Passport service.

.NET Passport Single Sign-in Service

- [What is Microsoft .NET Passport and what can I do with it?](#)
- [How does .NET Passport work?](#)
- [Where can I use .NET Passport?](#)
- [Does .NET Passport share my profile information with participating sites?](#)
- [How do I sign in to .NET Passport participating sites?](#)
- [Where can I register for a .NET Passport?](#)

.NET Passport Express Purchase and .NET Passport Wallet

- [What is .NET Passport express purchase?](#)
- [How do I use .NET Passport express purchase?](#)
- [What is the .NET Passport wallet?](#)
- [What personal information is stored in my .NET Passport wallet?](#)

Kids Passport

- [What is Kids Passport?](#)
- [How does a Kids Passport account work?](#)

Security and Privacy

- [How secure is .NET Passport?](#)
- [What about the privacy of my information?](#)
- [What is the .NET Passport privacy statement?](#)
- [Why should I trust Microsoft with my information?](#)

Microsoft .NET Passport Single Sign-in Service

What is Microsoft .NET Passport and what can I do with it?

.NET Passport is an online service that makes it possible for you to use your e-mail address and a single password to sign in—securely—to any .NET Passport participating Web site or service.

With a .NET Passport, you can:

- Sign in to .NET Passport participating sites **using your e-mail address and a single password** so you don't have to remember a different sign-in name and password at every Web site.
- **Make faster, more secure online purchases** with [.NET Passport express purchase](#).

- **Protect and control online privacy for children** with [Kids Passport](#).

How does .NET Passport work?

With .NET Passport, you don't need to register a member name and password at each new site you visit—simply use the e-mail address and password that you registered as your .NET Passport to sign in to any participating site or service.

The information you register with .NET Passport is stored online, securely, in the .NET Passport database as your ".NET Passport profile." When you sign in to a .NET Passport participating site by typing your e-mail address and password in the .NET Passport sign-in box, .NET Passport confirms that:

- The e-mail address you typed is registered with .NET Passport.
- The password you typed is correct.

.NET Passport then notifies the site that you are who you say you are (that you have provided valid "sign-in credentials"), and you are given access to the participating site.

Once you sign in to one .NET Passport participating site during an Internet session, you can sign in to others simply by clicking the .NET Passport sign-in button on each site.

The .NET Passport sign-in button is generally found in the upper-right corner of the page and looks like this: 

Where can I use .NET Passport?

You can use your .NET Passport at any of these [.NET Passport participating sites](#). The list of participating sites is updated frequently, so you may want to check it often.

Does .NET Passport share my profile information with participating sites?

.NET Passport lets you choose how much—if any—of your .NET Passport profile information you want to share with participating sites when you sign in.

You can use the check boxes near the bottom of the 'Registration' page to choose which information to share. You can also change your profile-sharing options at any time after registration on the [.NET Passport Member Services](#) page.

For more information about sharing your profile information, please read the [Microsoft .NET Passport privacy statement](#).

How do I sign in to .NET Passport participating sites?

To sign in to a .NET Passport participating site:

- Click the .NET Passport sign-in button and type your e-mail address and the password you created when you registered for a .NET Passport.
—Or—
- At some participating sites, you can sign in by typing your e-mail address and password in the .NET Passport sign-in box on the site's home page.

After you've signed in using your .NET Passport once, you can sign in to other .NET Passport participating sites simply by clicking the .NET Passport sign-in button on that

site.

The .NET Passport sign-in button is usually found in the upper-right corner of the Web page, and looks like this: 

Where can I register for a .NET Passport?

You can register for a .NET Passport at www.passport.com or at any [.NET Passport participating site](#).

You may already have a .NET Passport. If you have an MSN® Hotmail® or MSN.com account, you already have a .NET Passport. You can use your e-mail address and password from either of those services to sign in wherever you see the .NET Passport sign-in button. 

[Back to top](#)

.NET Passport Express Purchase

What is .NET Passport express purchase?

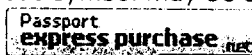
.NET Passport express purchase is a service that you can use to make purchases online by accessing the purchasing information held securely in your .NET Passport wallet.

A .NET Passport express purchase can be made only at [participating sites](#), and you must have a .NET Passport wallet to make a .NET Passport express purchase.

How do I use .NET Passport express purchase?

When you are ready to make a purchase at a participating site, click the .NET Passport express purchase button to access the payment, shipping, and billing information held in your .NET Passport wallet. That information is sent to the merchant securely, making it possible for you to complete the transaction without typing your payment information.

The .NET Passport express purchase symbol may be displayed as a button or a link.



Express purchase using .NET Passport

What is the .NET Passport wallet?

The .NET Passport wallet makes it possible for you to store credit card information and your shipping and billing addresses in a secure, online location. Only you have access to the information in your .NET Passport wallet.

When you're ready to make an online purchase at a participating .NET Passport express purchase site, you can access this information and send it to the merchant instantly and securely—without retyping your payment information.

You must register for a .NET Passport before you can create your .NET Passport wallet. If you already have a .NET Passport and want to create your .NET Passport wallet, go to [.NET Passport Member Services](#) and click the Create or edit my .NET Passport wallet

link.

What personal information is stored in my .NET Passport wallet?

The information stored in your .NET Passport wallet includes your credit card information and your shipping and billing addresses. This information is never sent to a participating site without your explicit consent.

You can store multiple cards and addresses in your wallet, and choose which ones to use for each purchase. Because this information is stored online, you don't have to retype it each time you buy something at a participating site.

Your .NET Passport wallet can store major credit cards, and debit cards that do not require a personal identification number (PIN).

[Back to top](#)

Microsoft Kids Passport

What is Kids Passport?

Kids Passport makes it possible for children to have their own .NET Passports while giving parents or guardians control over what .NET Passport profile information their children can share with participating Kids Passport sites.

Sites that offer the Kids Passport service may have areas that collect, use, or disclose children's personal information. With Kids Passport, parents can choose—on a site-by-site basis—what information a child can share with participating sites and services, and what the site can do with the information it does collect.

Kids Passport is not a Web filter that parents can use to keep their children from accessing specific sites.

How does a Kids Passport account work?

When a child tries to sign in to a participating site or service that requires personally identifiable information, the child must obtain consent from a parent or guardian before sharing that information.

The child can make this request directly through Kids Passport. The parent or guardian reviews the request and can either grant a specific level of consent, or deny consent altogether. In some cases, denying consent for a site to gather personally identifiable information will prevent a child from using the Web site.

[Back to top](#)

Security and Privacy

How secure is .NET Passport?

.NET Passport achieves a high level of Web security by using technologies and systems that are designed to prevent unauthorized access to your personal information. Here are the primary ways that .NET Passport protects your information:

- You must type your .NET Passport password to sign in to participating sites or to access your .NET Passport profile information. However, .NET Passport never

reveals your password to participating sites.

- .NET Passport uses industry-standard security technologies to encrypt your password, e-mail address, and .NET Passport wallet information whenever it's transmitted over the Internet.
- When making a .NET Passport express purchase, you can only access your .NET Passport wallet for a few minutes before you're required to retype your password.
- After several unsuccessful attempts to sign in, .NET Passport temporarily blocks further attempts. This makes it much more difficult for someone to guess your password using a password-cracking program.
- .NET Passport stores "cookies" (small text files) on your computer to enable you to sign in to participating sites. All .NET Passport cookies are encrypted. When you sign out of .NET Passport, all .NET Passport cookies are deleted from your computer.

What about the privacy of my information?

Microsoft is committed to protecting the privacy of people who use .NET Passport.

- Microsoft does not share the personal information in your .NET Passport profile with other companies without your consent.
- You may choose to have Microsoft share your .NET Passport profile information with other companies when you sign in to their .NET Passport-enabled sites. Sharing this information can make registration faster and lets sites offer you personalized services. You can indicate on the .NET Passport registration form, or in your .NET Passport profile following registration, which information to share.
- Sites that offer the .NET Passport service must display their own privacy statements and are bound by rules that require them to disclose how they use your .NET Passport information.
- If you have a .NET Passport wallet, your wallet information is never shared with participating sites at sign-in. Your .NET Passport wallet information is only shared when you choose which pieces to send to the merchant during a .NET Passport express purchase.

What is the .NET Passport privacy statement?

Your privacy is important to us. The .NET Passport privacy statement is based on the following fair information practices and enforcement principles that are widely endorsed by consumer privacy advocates, such as TRUSTe and BBBOnLine:

- **Notice** of how information will be used
- **Choice** about what information you want to share
- **Consent** to collection and distribution of personal information
- **Access** to personal information 24 hours a day, 7 days a week

For more information, please read the [Microsoft .NET Passport privacy statement](#).

Why should I trust Microsoft with my information?

In recent years, Microsoft has consistently been ranked as one of the most respected corporations in North America by the general public.

In addition, Microsoft has been a champion of Internet privacy standards and privacy organizations for many years.

More recently, Microsoft became a member of the Board of Directors for BBBOnLine and helped spearhead the global Online Privacy Alliance, a coalition of more than 80 global corporations and organizations working to promote consumer privacy online. Microsoft continues to work closely with government and consumer privacy groups worldwide.

[Back to top](#)

[For Consumers](#) | [For Business](#) | [For Press](#) | [International](#)

© 1999-2001 Microsoft Corporation. All rights reserved.
[TRUSTe Approved Privacy Statement](#) | [Terms of Use](#)



One password.

One easy way to
Sign in and Shop online.

- ▶ Look for the new .NET Passport button



Sign in at any participating .NET Passport, and then **sign in to other participating sites with a single click.** Read more about our new name.

- ▶ **Use ONE sign-in name and password** at all .NET Passport sites.
- ▶ **Store information in .NET Passport wallet** that will help you make faster, safer online purchases at any .NET Passport express purchase site.

And it's free!



Security

Use .NET Passport from any computer on the Internet. Your .NET Passport is protected by powerful online security technology, and a strict privacy policy. You control which sites access it.

Get your FREE .NET Passport today!

.NET Passport Q&A

Other great .NET Passport services:

- ▶ **Kids Passport** ★

Your kids can have their own .NET Passports and you control what information they share with participating sites.



Members

- ▶ Edit the information in your .NET Passport
- ▶ Reset your password
- ▶ Use your .NET Passport at these sites

Businesses

- ▶ Use .NET Passport on your Web site

International



.NET Passport around the world



Microsoft .NET Passport is Committed to Safeguarding Your Privacy

Microsoft® .NET Passport (" .NET Passport") recognizes that your privacy and the protection of your personal information is important to you. This statement discloses how we ensure that your personal information is protected while using the .NET Passport Web Site (www.passport.com), and while using the .NET Passport Services at participating web sites.

The .NET Passport Services include the following: .NET Passport sign-in, .NET Passport wallet and .NET Passport express purchase, and Kids Passport. By using the .NET Passport Web Site and the .NET Passport Services, you consent to the data practices described in this statement.

This statement includes an additional section that specifically describes our commitment to privacy for the Kids Passport service. You can read the [Kids Passport Privacy Statement](#) section below.

You should also familiarize yourself with the .NET Passport Terms of Use at <http://www.passport.com/Consumer/TermsOfUse.asp> before choosing to use the .NET Passport Services. For more information about how the .NET Passport Services work, visit <http://www.passport.com/Consumer/HowPassportWorks.asp>.

TRUSTe CERTIFICATION

Microsoft is a member of TRUSTe, an independent, non-profit initiative that exists to help people feel confident about using the Internet for communicating, shopping, researching, and living. TRUSTe aims to build this confidence by promoting the principles of disclosure and fair information practices among the web sites that participate in the program.

This Privacy Statement discloses the privacy practices for the .NET Passport Web Site and .NET Passport Services in accordance with the requirements of the TRUSTe Privacy Program. When you visit a web site displaying the TRUSTe trademark, you can expect to be notified of:

- What personally identifiable information of yours is collected.
- What organization is collecting the information.
- How the information is used.
- With whom the information may be shared.
- What choices are available to you regarding the collection, use, and distribution of the information.
- What kind of security procedures are in place to protect the loss, misuse, or alteration of information under the company's control.
- How you can correct any inaccuracies in the information.



Questions regarding this Privacy Statement should be directed to passpriv@microsoft.com. If any TRUSTe-certified web site, including this one, has not responded to your inquiry or your inquiry has not been satisfactorily addressed, please [contact TRUSTe](#).

COLLECTION AND STORAGE OF YOUR PERSONAL INFORMATION

During Registration

When you register for a .NET Passport account or a Kids Passport account, .NET Passport collects two kinds of information from you:

- **Personally identifiable information**, which is information that either personally identifies you or allows others to contact you. The personally identifiable information collected by .NET Passport includes your e-mail address, because your .NET Passport is based on your e-mail address. .NET Passport may also collect your name and/or phone number depending on which .NET Passport Services you register for.
- **Non-personally identifiable or "demographic" information**, which by itself does not identify you or allow others to contact you. The non-personally identifiable information that .NET Passport collects may include your country, state/region, ZIP/Postal Code, time zone, gender, birthday, and occupation.

If you choose to create a .NET Passport wallet, .NET Passport collects additional personally identifiable information, including your name, telephone number, credit card information, and billing and shipping addresses.

.NET Passport may also collect a secret question and secret answer that you provide. You use your secret question and answer to help verify your identity to .NET Passport if you need to reset your password.

You can register for a .NET Passport at a .NET Passport participating site or service, or at the .NET Passport Web Site (www.passport.com). The services you register for, and the amount and kind of information collected during registration, can vary depending on where you register.

If you register for a .NET Passport at a .NET Passport participating site or service, you will be opening two different accounts simultaneously:

- One with the participating site or service.
—And—
- One with .NET Passport.

You can then use your .NET Passport to sign in to that participating site and to all other .NET Passport participating sites and services.

Note Some .NET Passport participating sites may require you to open an MSN.com or Hotmail.com e-mail account when you register. These e-mail addresses are automatically registered as .NET Passports, so in this case you would be registering for:

- A .NET Passport.
- An account at the .NET Passport participating site or service.
—And—
- Free e-mail services through MSN.com or Hotmail.com.

Not all of the information you provide during registration at a participating site will be stored by .NET Passport. Some information (for example, clothing sizes or music preferences) may be specific to—and stored by—the participating site or service. If a .NET Passport participating site uses a single registration form to collect both .NET Passport information and site-specific information, the information stored by .NET Passport will be identified on the form by a .NET Passport icon next to each field.

If you register at the .NET Passport Web Site, you will simply be registering for a .NET Passport. All of the information you provide when you register at the .NET Passport Web Site will be stored by .NET Passport.

The information collected by .NET Passport—which may include your e-mail address, name, country, state/region, ZIP/Postal Code, time zone, gender, birthday, and occupation—comprise your .NET Passport "profile." You can access and edit your .NET Passport profile at any time after

registration by going to .NET Passport Member Services at <http://memberservices.passport.com> and clicking the Edit my .NET Passport profile link.

When Signing In

When you use your .NET Passport to sign in to other .NET Passport participating sites, some of those sites may collect additional information from you so you can register with them as well.

You should review the privacy statement for each .NET Passport participating site you register with to determine how each site or service will use the information it collects.

The .NET Passport Wallet

If you also create a .NET Passport wallet, your .NET Passport wallet information is stored separately from your .NET Passport profile. You can access and edit your .NET Passport wallet information by going to .NET Passport Member Services at <http://memberservices.passport.com> and clicking the Create or edit my .NET Passport wallet link.

General

Personally identifiable information that you provide to .NET Passport may be stored and processed in the United States or any other country in which Microsoft or its affiliates, subsidiaries, or agents maintain facilities. By using the .NET Passport Services, you consent to any such transfer of information outside of your country.

USE OF YOUR PERSONAL INFORMATION

.NET Passport will not share, sell, or use your personal information in a manner that differs from what is described in this Privacy Statement, unless we have your consent.

.NET Passport uses the information for the operation and maintenance of your .NET Passport account and the .NET Passport Services.

.NET Passport sends you a welcome e-mail message when you first register, informing you about the service and telling you how to manage your .NET Passport account. .NET Passport may also send you periodic updates or surveys related to the .NET Passport Services. These e-mails are considered essential to the provision of the service you have requested. You are not able to choose to unsubscribe to these mailings, but you may choose not to participate in the surveys.

.NET Passport also occasionally hires other companies to provide limited services on our behalf, such as answering customer support inquiries or performing statistical analyses of our services. .NET Passport will only provide those companies the information they need to deliver the services, and they are prohibited from using that information for any other purpose.

From time to time, .NET Passport may report average age, gender, and other aggregate membership statistics to our participating sites. These reports will not include personal information that identifies you or allows others to contact you.

.NET Passport will disclose personal information if required to do so by law or in the good-faith belief that such action is necessary to:

- a. Conform to legal requirements or comply with legal process served on Microsoft.
- b. Protect and defend the rights or property of Microsoft, .NET Passport, or .NET Passport participating sites.
- c. Enforce the Terms of Use.
- Or—
- d. Act under exigent circumstances to protect the personal safety of users of Microsoft, the .NET Passport Web Site, or the public.

.NET Passport participating sites and services with whom you choose to share the information can use it for a variety of purposes. These can include personalizing your experience at their sites and reducing registration time by using information in your .NET Passport account to pre-fill their registration forms. **We recommend that you review the privacy statement at each .NET Passport participating site before you share your personal information with them.**

CONTROL OF YOUR PERSONAL INFORMATION

You control which .NET Passport participating sites and services receive the information in your .NET Passport profile and .NET Passport wallet. The information stored by .NET Passport is not shared with a .NET Passport participating site or service unless you explicitly choose to provide it by clicking the .NET Passport sign-in link or the .NET Passport express purchase button on that site. It is important for you to read the privacy statement and terms of use for each .NET Passport participating site or service you visit before you sign in or make a .NET Passport express purchase, so that you understand how the site may use your .NET Passport information.

Some of your .NET Passport information is never shared with any .NET Passport participating site. This includes your password, your .NET Passport security key (which you can only get by visiting a site that uses this service), and your secret question and secret answer.

Your .NET Passport Profile

You can decide which pieces of information in your .NET Passport profile to share with the .NET Passport participating sites that you sign in to. You can use the check boxes on the 'Registration' page and the 'Edit Your .NET Passport Profile' page to choose whether to share your e-mail address, your name, and other profile information.

There are two specific cases, however, in which a .NET Passport participating site will receive your profile information (except your password and secret question and secret answer) regardless of your check-box settings:

- The participating site where you registered for your .NET Passport will receive the profile information you provided during registration.
- If you registered an @msn.com, @hotmail.com, @webtv.net, or @compaq.net .NET Passport, then those e-mail domains will always receive your profile information when you visit their sites.

In general, the e-mail address associated with your .NET Passport account is not shared with .NET Passport participating sites or services. However, a few sites currently require your e-mail address in order to provide you their services. (For example, Hotmail requires your e-mail address to provide your requested e-mail services.) In those cases, .NET Passport will provide your e-mail address to those sites when you sign in to them.

The .NET Passport Wallet

You control which pieces of information in your .NET Passport wallet are shared with .NET Passport express purchase participating sites and services on a per-transaction basis. After clicking the .NET Passport express purchase button at a participating site, you will be able to choose which credit card and billing and shipping address information to send to the participating site for that purchase.

Other Information

Some sites need additional .NET Passport information to operate your account properly. This "operational" information is shared automatically with the participating site or service when you sign in using your .NET Passport.

Operational information does not include the personal information that you provide as part of your .NET Passport profile, and it is shared with the site regardless of whether you choose to share your profile information with the site when you sign in.

The operational information shared at sign-in includes:

- The version number .NET Passport assigns to your profile. (A new number is assigned each time you change your .NET Passport profile to tell participating sites that the information has been updated. Your personal .NET Passport profile information is not shared without your permission.)
—Also, whether—
- Your e-mail address has been verified.
- Your account has been deactivated.
- Your account is a Kids Passport account.
- Your account has an associated .NET Passport wallet.
- You have consented to be listed in the Hotmail member directory or other public directories.

ACCESS TO YOUR PERSONAL INFORMATION

You can always add, update, or make other changes to the information in your .NET Passport profile or .NET Passport wallet by visiting .NET Passport Member Services at <http://memberservices.passport.com>.

SECURITY OF YOUR PERSONAL INFORMATION

Your .NET Passport information is stored on secure .NET Passport servers that are protected in controlled facilities. You must type the correct password to access your .NET Passport information, and your password is never shared with .NET Passport participating sites.

When you request to have your .NET Passport information sent to a .NET Passport participating site, .NET Passport uses industry-standard security technologies to encrypt it for secure transmission over the Internet.

MANAGED .NET PASSPORTS

If you received your .NET Passport from someone else, without registering for it yourself, your .NET Passport may belong to a "managed domain." In a managed domain, the administrator of a company with whom you have a business relationship (for example, your employer) can create your .NET Passport for you, including your .NET Passport e-mail address and password. You can use the .NET Passport much like any other .NET Passport. The company administrator, however, has control over the .NET Passport and can edit your .NET Passport profile, reset your password, and manage the .NET Passport account without your permission.

USE OF A UNIQUE ID

.NET Passport associates a .NET Passport unique identifier with every .NET Passport account at registration. The unique identifier is a unique 64-bit number that .NET Passport sends (encrypted) to each .NET Passport participating site that you choose to sign in to. This unique identifier makes it possible for the site to determine whether you are the same person from one sign-in session to the next. It can also allow you to personalize your experience at a site, even if you choose to sign in anonymously (that is, to not share your e-mail address, name, or any of your other .NET Passport profile data).

USE OF COOKIES

A cookie is a very small text file that a web site saves to your computer's hard disk to store information that you provide about yourself or to store your preferences. .NET Passport uses cookies whenever you sign in to a .NET Passport participating site. .NET Passport stores your unique identifier, the time you signed in, and whatever .NET Passport profile information you have chosen to share with participating sites, in a secure, encrypted cookie on your hard disk. The cookie allows you to move from page to page at the participating site without having to sign in again on each page.

You have the ability to accept or decline cookies using the settings on your browser. If you choose to decline cookies, you will not be able to sign in using your .NET Passport.

When you sign out of .NET Passport, all .NET Passport-related cookies from all .NET Passport participating sites are deleted from your computer. However, the sites you visited may store their own cookies on your computer, and these may persist after you sign out of .NET Passport. .NET Passport recommends that you read each participating site's privacy statement to understand their policies and practices.

.NET PASSPORT PARTICIPATING SITES' USE OF YOUR PERSONAL INFORMATION

To become a .NET Passport participating site, web sites must agree to protect your personal information. All participating sites are required to have a posted privacy statement and to use commercially reasonable efforts to comply with industry-standard privacy guidelines and practices. And all U.S.-based sites are encouraged (but not required) to be registered with an independent, industry-recognized, privacy assurance organization such as [TRUSTe](#) or [BBBOnLine](#).

Nevertheless, the privacy practices of .NET Passport participating sites will vary. **Therefore you should carefully review the privacy statement for each .NET Passport participating site you sign in to, in order to determine how each site or service will use the information it collects.**

If .NET Passport becomes aware of ongoing, site-specific issues with a .NET Passport participating site, we will work to address those issues with the site. If at any time you believe that a .NET Passport participating site has not adhered to these principles, please notify .NET Passport by e-mail at passpriv@microsoft.com.

CHANGES TO THIS PRIVACY STATEMENT

.NET Passport will occasionally update this Privacy Statement. When we do, we will also revise the "last updated" date at the bottom of the Privacy Statement. For material changes to this Privacy Statement, .NET Passport will notify you by placing a prominent notice on the .NET Passport Web Site. .NET Passport encourages you to periodically review this Privacy Statement to stay informed about how we are protecting your information. Your continued use of the .NET Passport Services constitutes your agreement to this Privacy Statement.

ENFORCEMENT OF THIS PRIVACY STATEMENT

As a licensee of TRUSTe, and upholding our commitment to protecting the privacy of your personal information, .NET Passport has agreed to disclose its information practices and to have its privacy practices reviewed for compliance by TRUSTe. If you have questions regarding this statement, you should first contact .NET Passport by sending an e-mail message to:

passpriv@microsoft.com

If you do not receive acknowledgment of your inquiry or your inquiry has not been addressed to your satisfaction, you should then contact TRUSTe at:

www.truste.org/users/users_watchdog.html

TRUSTe will serve as a liaison with .NET Passport to resolve your concerns.

CONTACT INFORMATION

If you have questions regarding .NET Passport or this Privacy Statement, or if you have a problem with a .NET Passport participating site, please send an e-mail message to:

passpriv@microsoft.com

You can also contact .NET Passport by postal mail at:

Microsoft .NET Passport Privacy
Microsoft Corporation
One Microsoft Way
Redmond, Washington 98052

.NET Passport will use all commercially reasonable efforts to promptly determine and correct the problem.

Microsoft Kids Passport Privacy Statement

Microsoft is especially concerned about the safety and protection of children's personal information collected and used online. Microsoft Kids Passport ("Kids Passport") allows parents to consent to the collection, use, and sharing of their children's information with .NET Passport participating sites and services that have agreed to use Kids Passport as their parental consent process.

Note Kids Passport is currently available only in the United States, but we plan to make it available in other countries in the future.

CHILDREN'S ACCESS TO SITES WITHOUT PARENTAL CONSENT

.NET Passport participating sites and services that utilize Kids Passport may have areas that are accessible to all users, including children, as well as areas that require parental consent because they collect, use, or disclose the personal information of children. If your child tries to access an area of these sites or services that does not collect any personal information (and therefore does not require parental consent), the site may permit your child to access these areas.

If your child tries to access an area that does collect, use, or disclose personal information, the site may either display a new page that directs your child to an area of the site that does not require parental consent, or display an error page that tells your child that they need a parent's permission to use this area of the web site. This page will also direct them to the Kids Passport site, where there are instructions on how to obtain parental consent.

COLLECTION OF CHILDREN'S PERSONAL INFORMATION

When you register your child for a Kids Passport, you will be asked to provide your child's birth date, sign-in name, password, password reset question and answer, e-mail address, country, and state or region. You will also be given the opportunity to control the sharing of e-mail address, name, and other registration information.

If your child registers for a .NET Passport on his or her own, .NET Passport will collect the information normally collected from individuals who register for a .NET Passport with the participating site. If any participating site asks .NET Passport to collect your child's age, and the age your child enters qualifies him or her as a child, then your child will be blocked from using his or her .NET Passport until you provide your consent. Unless you provide your consent, the participating site will receive none of the information your child entered during registration.

USE OF CHILDREN'S PERSONAL INFORMATION BY .NET PASSPORT

When you create a Kids Passport, the information you provide is stored in your child's .NET Passport profile. .NET Passport uses this information to operate its services, as described above, in the [.NET Passport Privacy Statement](#). By creating a Kids Passport you are consenting to the collection, use, and disclosure of the information in your child's .NET Passport profile as described in this statement.

.NET Passport does not share the information contained in your child's .NET Passport Profile with third parties, except for .NET Passport participating sites where you have consented to such sharing, or as otherwise disclosed in this statement.

USE OF CHILDREN'S PERSONAL INFORMATION BY .NET PASSPORT PARTICIPATING SITES AND SERVICES

Kids Passport shares your child's information with participating sites and services in accordance with the consent you have given for your child's Kids Passport account.

These .NET Passport participating sites provide a variety of products and services to online users. All of these sites agree to have a posted privacy statement describing how they use personal information collected by their web site.

For more information, you can view the current list of [Kids Passport participating sites and services](#). These .NET Passport participating sites will not collect, use, or disclose your child's information except in accordance with your consent decisions.

CONTROL OF CHILDREN'S PERSONAL INFORMATION

Kids Passport allows you to limit the amount of information shared with the sites and services participating in the Kids Passport program. You can choose to allow .NET Passport to share all information in your child's .NET Passport profile with a participating site or service, or you can limit the information shared to just a unique identifier and an age range.

Kids Passport also allows you to choose, on site-by-site basis, up to three types of consent for how Kids Passport participating sites and services will collect, use, and disclose your child's personal information.

- You can choose "deny," which instructs the site to deny access to areas of the site or service that require the collection or permit the disclosure of personal information.
- You can give "limited consent," which means that you consent to the information being used for the operation of the site or service, including personalization, but not sharing it with any other third parties, except as necessary to operate the site or service.
- You can give "full consent," which means that you consent to the information being used for the operation of the site, for personalization and for sharing the information with other third parties.

Not all participating sites and services offer all three levels of consent. For example, some sites and services (such as e-mail or chat services) inherently involve the potential sharing of personal information with third parties, so the "limited consent" option would, in effect, deny access to the service. In such cases, the site may offer only the "full" and "deny" consent options.

For more information, you can view the current list of [Kids Passport participating sites and services](#). It is important that you read the privacy statement and terms of use for each web site you are granting consent to.

VERIFICATION OF PARENTAL CONSENT

A valid credit card number helps .NET Passport verify that you are an adult. Kids Passport obtains and verifies parental consent through the use of a credit card validation process. There is no charge to your credit card. This process checks that the credit card number is valid and validates address information.

SECURITY OF CHILDREN'S PERSONAL INFORMATION

Your child's Kids Passport information is stored on secure Microsoft servers that are protected in controlled facilities. When your child requests to have their Kids Passport information sent to a .NET Passport participating site or service—in accordance with the level of consent you have granted—the information is encrypted and securely sent to that web site using advanced encryption technology.

ACCESSING AND UPDATING YOUR CHILD'S PERSONAL INFORMATION

You can change, edit, update, or delete the information in your child's Kids Passport account at any time. To update your child's account information (including updating your child's preferences and changing your consent level for individual web sites), visit Kids Passport at <http://kids.passport.com> and click Parent's Point. You can also make changes to the list of web sites you have previously granted consent to.

CONTACT INFORMATION

If you have questions regarding Kids Passport or this Privacy Statement, please send an e-mail message to:

passpriv@microsoft.com

You can also contact .NET Passport by postal mail at:

KIDS Passport
Microsoft Corporation
One Microsoft Way
Redmond, Washington 98052

Last Updated: October 8, 2001

[For Consumers](#) | [For Business](#) | [For Press](#) | [International](#)

© 1999-2001 Microsoft Corporation. All rights reserved.
[TRUSTe Approved Privacy Statement](#) | [Terms of Use](#)



[Passport Home](#) | [Kids Passport](#) | [Member Services](#) | [Site Directory](#) | [Privacy Policy](#) | [Help](#) | [Passport sign in](#) 

[Parents' Point](#)

[Kids' Corner](#)

[Kids Passport Help](#)

[Kids Privacy Policy](#)

Welcome to Kids Passport

..... Helping parents protect their children's privacy online.



Parents' Point

Set up and edit accounts, or review and complete requests for consent.



Kids' Corner

Request permission to use sites, and view your pending requests.

Kids Site Directory

See the participating sites.



Kids Passport Help

Find the answer to your question.



Learn about the Children's Online Privacy Protection Act

Discover how Kids Passport is helping parents to keep their child's identity safe online.

[Help](#) | [What is Kids Passport](#) | [Where can I use Passport?](#) | [International](#)

© 1999-2001 Microsoft Corporation. All rights reserved.
[TRUSTe Approved Privacy Statement](#) | [Terms of Use](#)



Get a Passport for your child

Please read this important information, and then fill out the registration form below.

Microsoft® Kids Passport is a free service that helps you conveniently protect and control your children's online privacy. Today, many Web sites routinely collect personal information. With Kids Passport, you can grant or deny consent to participation Web sites (including the Microsoft family of Web sites) to collect personal information from your children. In addition, you can make specific choices for each child and for each site, all in one convenient, centralized location.

Follow these simple steps to set up a Kids Passport account for your child:

1. Fill out the registration form below to provide us with the following personal information: your child's sign-in name and password, an e-mail address for you or your child; and your child's date of birth. We are also asking you for some additional information to make it easier to reset the password if your child forgets it. Your child's Kids Passport does not include the wallet service.
2. Provide consent to Passport to collect, use, and/or disclose this information to participating sites your child signs in to.
3. Verify you are an adult by creating a Passport wallet and providing a valid credit card number. (The credit card is for verification purposes only, you will not be charged.)

To learn more about the Kids Passport information practices, read the [Kids Privacy Policy](#). To learn more about the new federal law that protects children's personal information online, see the [Children's Online Privacy Protection Act](#).

Step 1 of 3: Get a Passport for your child

Parents: Fill out the registration form below with information about your child.

Fields marked with  will be stored in your Passport.

[Help](#)

Child's Sign-in Name	_____@passport.com 
Child's Password	_____  Six-character minimum; no spaces
Retype Child's Password	_____ 
Child's Birth Date	Month ____ Day ____ (e.g., 1999)  Passport requires your birth date to comply with current law.



Tired of registration forms? You can speed registration and get personalized services at participating Microsoft Passport sites by sharing your Passport information with them when you sign in. Check the boxes below to choose how much of your Passport information Microsoft can share with other companies' Passport sites at sign-in:

- ☐ Share my e-mail address
☐ Share my other registration information

[More about Passport, privacy, and security](#)



[Member Services](#) [Terms of Use](#) [Privacy Statement](#)

Some elements © 1999 - 2001 Microsoft® Corporation. All rights reserved.

Microsoft Kids Passport Privacy Statement

Microsoft is especially concerned about the safety and protection of children's personal information collected and used online. Microsoft Kids Passport ("Kids Passport") allows parents to consent to the collection, use, and sharing of their children's information with Passport participating sites and services that have agreed to use Kids Passport as their parental consent process.

Note Kids Passport is currently available only in the United States, but we plan to make it available in other countries in the future.

CHILDREN'S ACCESS TO SITES WITHOUT PARENTAL CONSENT

Passport participating sites and services that utilize Kids Passport may have areas that are accessible to all users, including children, as well as areas that require parental consent because they collect, use, or disclose the personal information of children. If your child tries to access an area of these sites or services that does not collect any personal information (and therefore does not require parental consent), the site may permit your child to access these areas.

If your child tries to access an area that does collect, use, or disclose personal information, the site may either display a new page that directs your child to an area of the site that does not require parental consent, or display an error page that tells your child that they need a parent's permission to use this area of the web site. This page will also direct them to the Kids Passport site, where there are instructions on how to obtain parental consent.

COLLECTION OF CHILDREN'S PERSONAL INFORMATION

When you register your child for a Kids Passport, you will be asked to provide your child's birth date, sign-in name, password, password reset question and answer, e-mail address, country, and state or region. You will also be given the opportunity to control the sharing of e-mail address, name, and other registration information.

If your child registers for a Passport on his or her own, Passport will collect the information normally collected from individuals who register for a Passport with the participating site. If any participating site asks Passport to collect your child's age, and the age your child enters qualifies him or her as a child, then your child will be blocked from using his or her Passport until you provide your consent. Unless you provide your consent, the participating site will receive none of the information your child entered during registration.

USE OF CHILDREN'S PERSONAL INFORMATION BY PASSPORT

When you create a Kids Passport, the information you provide is stored in your child's Passport profile. Passport uses this information to operate its services, as described above, in the Passport [Privacy Statement](#). By creating a Kids Passport you are consenting to the collection, use, and disclosure of the information in your child's Passport profile as described in this statement.

Passport does not share the information contained in your child's Passport Profile with third parties, except for Passport participating sites where you have consented to such sharing, or as otherwise disclosed in this statement.

USE OF CHILDREN'S PERSONAL INFORMATION BY PASSPORT PARTICIPATING SITES AND SERVICES

Kids Passport shares your child's information with participating sites and services in accordance with the consent you have given for your child's Kids Passport account.

These Passport participating sites provide a variety of products and services to online users. All of

these sites agree to have a posted privacy statement describing how they use personal information collected by their web site.

For more information, you can view the current list of Kids Passport participating sites and services. These Passport participating sites will not collect, use, or disclose your child's information except in accordance with your consent decisions.

CONTROL OF CHILDREN'S PERSONAL INFORMATION

Kids Passport allows you to limit the amount of information shared with the sites and services participating in the Kids Passport program. You can choose to allow Passport to share all information in your child's Passport profile with a participating site or service, or you can limit the information shared to just a unique identifier and an age range.

Kids Passport also allows you to choose, on site-by-site basis, up to three types of consent for how Kids Passport participating sites and services will collect, use, and disclose your child's personal information.

- You can choose "deny," which instructs the site to deny access to areas of the site or service that require the collection or permit the disclosure of personal information.
- You can give "limited consent," which means that you consent to the information being used for the operation of the site or service, including personalization, but not sharing it with any other third parties, except as necessary to operate the site or service.
- You can give "full consent," which means that you consent to the information being used for the operation of the site, for personalization and for sharing the information with other third parties.

Not all participating sites and services offer all three levels of consent. For example, some sites and services (such as e-mail or chat services) inherently involve the potential sharing of personal information with third parties, so the "limited consent" option would, in effect, deny access to the service. In such cases, the site may offer only the "full" and "deny" consent options.

For more information, you can view the current list of Kids Passport participating sites and services. It is important that you read the privacy statement and terms of use for each web site you are granting consent to.

VERIFICATION OF PARENTAL CONSENT

A valid credit card number helps Passport verify that you are an adult. Kids Passport obtains and verifies parental consent through the use of a credit card validation process. There is no charge to your credit card. This process checks that the credit card number is valid and validates address information.

SECURITY OF CHILDREN'S PERSONAL INFORMATION

Your child's Kids Passport information is stored on secure Microsoft servers that are protected in controlled facilities. When your child requests to have their Kids Passport information sent to a Passport participating site or service—in accordance with the level of consent you have granted—the information is encrypted and securely sent to that web site using advanced encryption technology.

ACCESSING AND UPDATING YOUR CHILD'S PERSONAL INFORMATION

You can change, edit, update, or delete the information in your child's Kids Passport account at any time. To update your child's account information (including updating your child's preferences and changing your consent level for individual web sites), visit Kids Passport at <http://kids.passport.com> and click Parent's Point. You can also make changes to the list of web sites you have previously granted consent to.

CONTACT INFORMATION

If you have questions regarding Kids Passport or this Privacy Statement, please send an e-mail message to:

passpriv@microsoft.com

You can also contact Passport by postal mail at:

KIDS Passport
Microsoft Corporation
One Microsoft Way
Redmond, Washington 98052

Last Updated: August 15, 2001

For Consumers | For Business | For Press | International

© 1999-2001 Microsoft Corporation. All rights reserved.
TRUSTe Approved Privacy Statement | Terms of Use

Decision and Order

DECISION AND ORDER

The Federal Trade Commission having initiated an investigation of certain acts and practices of the respondent named in the caption hereof, and the respondent having been furnished thereafter with a copy of a draft complaint that the Bureau of Consumer Protection proposed to present to the Commission for its consideration and which, if issued by the Commission, would charge the respondent with violation of the Federal Trade Commission Act, 15 U.S.C. § 45 et seq; and

The respondent, its attorney, and counsel for the Commission having thereafter executed an agreement containing a consent order, an admission by the respondent of all the jurisdictional facts set forth in the aforesaid draft complaint, a statement that the signing of said agreement is for settlement purposes only and does not constitute an admission by respondent that the law has been violated as alleged in such complaint, or that the facts as alleged in such complaint, other than jurisdictional facts, are true, and waivers and other provisions as required by the Commission's Rules.

The Commission having thereafter considered the matter and having determined that it has reason to believe that the respondent has violated the said Acts and Regulations, and that a complaint should issue stating its charges in that respect, and having thereupon accepted the executed consent agreement and placed such agreement on the public record for a period of thirty (30) days, and having duly considered the comments received, now in further conformity with the procedure described in § 2.34 of its Rules, the Commission hereby issues its complaint, makes the following jurisdictional findings and enters the following order:

1. Respondent Microsoft is a Washington corporation with its principal office or place of business at One Microsoft Way, Redmond, Washington 98052.

Decision and Order

2. The Federal Trade Commission has jurisdiction of the subject matter of this proceeding and of the respondent, and the proceeding is in the public interest.

ORDER

DEFINITIONS

For purposes of this order, the following definitions shall apply:

1. “Personally identifiable information” or “personal information” shall mean individually identifiable information from or about an individual including, but not limited to: (a) a first and last name; (b) a home or other physical address, including street name and name of city or town; (c) an email address or other online contact information, such as an instant messaging user identifier or a screen name that reveals an individual’s email address; (d) a telephone number; (e) a Social Security Number; (f) a persistent identifier, such as a customer number held in a “cookie” or processor serial number, that is combined with other available data that identifies an individual; or (g) any information that is combined with any of (a) through (f) above.
2. “Covered online service” shall mean Passport, Kids Passport, Passport Wallet, any substantially similar product or service, or any multisite online authentication service.
3. Unless otherwise specified, “respondent” shall mean Microsoft Corporation, its successors and assigns and its officers, agents, representatives, and employees acting within the scope of their authority on behalf of, or in active concert or participation with Microsoft Corporation.
4. “Commerce” shall mean as defined in Section 4 of the Federal Trade Commission Act, 15 U.S.C. § 44.

Decision and Order

I.

IT IS ORDERED that respondent, directly or through any corporation, subsidiary, division, or other device, in connection with the advertising, marketing, promotion, offering for sale, or sale of a covered online service, in or affecting commerce, shall not misrepresent in any manner, expressly or by implication, its information practices, including:

- A. what personal information is collected from or about consumers;
- B. the extent to which respondent's product or service will maintain, protect or enhance the privacy, confidentiality, or security of any personally identifiable information collected from or about consumers;
- C. the steps respondent will take with respect to personal information it has collected in the event that it changes the terms of the privacy policy in effect at the time the information was collected;
- D. the extent to which the service allows parents to control what information their children can provide to participating sites or the use of that information by such sites; and
- E. any other matter regarding the collection, use, or disclosure of personally identifiable information.

II.

IT IS FURTHER ORDERED that respondent, and its successors and assigns, in connection with the advertising, marketing, promotion, offering for sale, or sale of a covered online service, in or affecting commerce, shall establish and maintain a comprehensive information security program in writing that is reasonably designed to protect the security, confidentiality, and integrity of personal information collected from or about

Decision and Order

consumers. Such program shall contain administrative, technical, and physical safeguards appropriate to respondent's size and complexity, the nature and scope of respondent's activities, and the sensitivity of the personal information collected from or about consumers, including:

- A. The designation of an employee or employees to coordinate and be accountable for the information security program.
- B. The identification of material internal and external risks to the security, confidentiality, and integrity of customer information that could result in the unauthorized disclosure, misuse, alteration, destruction, or other compromise of such information, and assessment of the sufficiency of any safeguards in place to control these risks. At a minimum, this risk assessment should include consideration of risks in each area of relevant operation, including: (1) employee training and management; (2) information systems, including network and software design, information processing, storage, transmission and disposal; and (3) prevention, detection, and response to attacks, intrusions, or other systems failures.
- C. Design and implementation of reasonable safeguards to control the risks identified through risk assessment, and regular testing or monitoring of the effectiveness of the safeguards' key controls, systems, and procedures.
- D. Evaluation and adjustment of respondent's information security program in light of the results of the testing and monitoring required by paragraph C, any material changes to respondent's operations or business arrangements, or any other circumstances that respondent knows or has reason to know may have a material impact on its information security program.

Decision and Order

III.

IT IS FURTHER ORDERED that respondent obtain within one (1) year, and on a biannual basis thereafter, an assessment and report from a qualified, objective, independent third-party professional, using procedures and standards generally accepted in the profession, that certifies:

- A. that respondent has in place a security program that provides protections that meet or exceed the protections required by Part II of this order; and
- B. that respondent's security program is operating with sufficient effectiveness to provide reasonable assurance that the security, confidentiality, and integrity of consumer's personal information has been protected.

The report required by this paragraph shall be prepared by a Certified Information System Security Professional (CISSP) or by a person or organization approved by the Associate Director for Enforcement, Bureau of Consumer Protection, Federal Trade Commission.

IV.

IT IS FURTHER ORDERED that respondent, and its successors and assigns, shall for a period of five (5) years after the date of service of this order maintain and upon request make available to the Federal Trade Commission for inspection and copying a print or electronic copy of the following documents relating to compliance with this order:

- A. a sample copy of each different print, broadcast, cable, or Internet advertisement, promotion, information collection form, Web page, screen, email message, or other document containing any representation to consumers regarding respondent's collection, use, and security of personal information from or about consumers. Each Web page copy

Decision and Order

shall be dated and contain the full URL of the Web page where the material was posted online. Electronic copies shall include all text and graphics files, audio scripts, and other computer files used in presenting the information on the Web. Provided, however, that after creation of any Web page or screen in compliance with this order, respondent shall not be required to retain a print or electronic copy of any amended Web page or screen to the extent that the amendment does not affect respondent's compliance obligations under this order;

- B. all plans, reports, studies, reviews, audits, audit trails, policies, and training materials, whether prepared by or on behalf of respondent, relating to respondent's compliance with this order; and
- C. any documents, whether prepared by or on behalf of respondent, that contradict, qualify, or call into question respondent's compliance with this order.

V.

IT IS FURTHER ORDERED that respondent, and its successors and assigns, shall deliver a copy of this order to all current and future principals, officers, directors, and managers, and to all current and future employees, agents, and representatives having managerial responsibilities relating to the subject matter of this order. Respondent shall deliver this order to such current personnel within thirty (30) days after the date of service of this order, and to such future personnel within thirty (30) days after the person assumes such position or responsibilities.

VI.

IT IS FURTHER ORDERED that respondent Microsoft Corporation, and its successors and assigns, shall notify the Commission at least thirty (30) days prior to any change in the

Decision and Order

corporation that may affect compliance obligations arising under this order, including, but not limited to, a dissolution, assignment, sale, merger, or other action that would result in the emergence of a successor corporation; the creation or dissolution of a subsidiary, parent, or affiliate that engages in any acts or practices subject to this order; the proposed filing of a bankruptcy petition; or a change in the corporate name or address. Provided, however, that, with respect to any proposed change in the corporation about which respondent learns less than thirty (30) days prior to the date such action is to take place, respondent shall notify the Commission as soon as is practicable after obtaining such knowledge. All notices required by this Part shall be sent by certified mail to the Associate Director, Division of Enforcement, Bureau of Consumer Protection, Federal Trade Commission, Washington, D.C. 20580.

VII.

IT IS FURTHER ORDERED that respondent Microsoft Corporation, and its successors and assigns, shall within sixty (60) days after service of this order, and at such other times as the Federal Trade Commission may require, file with the Commission a report, in writing, setting forth in detail the manner and form in which they have complied with this order.

VIII.

This order will terminate on December 20, 2022, or twenty (20) years from the most recent date that the United States or the Federal Trade Commission files a complaint (with or without an accompanying consent decree) in federal court alleging any violation of the order, whichever comes later; provided, however, that the filing of such a complaint will not affect the duration of:

A. Any Part in this order that terminates in less than twenty (20) years;

Decision and Order

- B. This order's application to any respondent that is not named as a defendant in such complaint; and
- C. This order if such complaint is filed after the order has terminated pursuant to this Part.

Provided, further, that if such complaint is dismissed or a federal court rules that the respondent did not violate any provision of the order, and the dismissal or ruling is either not appealed or upheld on appeal, then the order will terminate according to this Part as though the complaint had never been filed, except that the order will not terminate between the date such complaint is filed and the later of the deadline for appealing such dismissal or ruling and the date such dismissal or ruling is upheld on appeal.

By the Commission.

Analysis

Analysis of Proposed Consent Order to Aid Public Comment

The Federal Trade Commission has accepted, subject to final approval, an agreement containing a consent order from Microsoft Corporation (“Microsoft”).

The proposed consent order has been placed on the public record for thirty (30) days for receipt of comments by interested persons. Comments received during this period will become part of the public record. After thirty (30) days, the Commission will again review the agreement and the comments received, and will decide whether it should withdraw from the agreement and take appropriate action or make final the agreement's proposed order.

Microsoft develops, manufactures, licenses, and supports a myriad of software products, sells hardware devices, provides consulting services, trains and certifies system developers, and offers a variety of online services. This matter concerns allegedly false or misleading representations made in connection with three related Microsoft services: the Passport Single Sign-In service (“Passport”); Passport Express Purchase (generally referred to as “Passport Wallet”); and Kids Passport (referred to collectively as the “Passport services”). Passport is an online authentication service that allows consumers to sign in at multiple Web sites with a single username and password. Passport Wallet and Kids Passport are add-on services that provide online purchasing and parental consent services.

The Commission’s proposed complaint alleges that Microsoft misrepresented:

- (1) that it maintained a high level of online security by employing sufficient measures reasonable and appropriate under the circumstances to maintain and protect the privacy and confidentiality of personal information obtained from or about consumers in connection with the Passport and Passport Wallet services;

Analysis

- (2) that purchases made at a Passport Express Purchase site with Passport Wallet are safer or more secure than purchases made at the same Passport Express Purchase site without using the Passport Wallet;
- (3) that Passport did not collect any personally identifiable information other than that described in its privacy policy, when, in fact, Passport collected, and maintained for a limited period of time, a personally identifiable record of the sites to which a Passport user signed in, along with the dates and times of sign in, which customer service representatives linked to a user's name in order to respond to a user's request for service; and
- (4) that the Kids Passport service provided parents with control over the information their children could provide to participating Passport sites and the use of that information by such sites.

The proposed consent order applies to the collection and storage of personal information from or about consumers in connection with the advertising, marketing, promotion, offering for sale, or sale of Passport, Kids Passport, Passport Wallet, any substantially similar product or service, or any multisite online authentication service. It contains provisions designed to prevent Microsoft from engaging in practices similar to those alleged in the complaint in the future.

Specifically, Part I of the proposed order prohibits misrepresentations regarding Microsoft's information practices, including:

- what personal information is collected from or about consumers;
- the extent to which respondent's product or service will maintain, protect or enhance the privacy, confidentiality, or

Analysis

security of any personally identifiable information collected from or about consumers;

- the steps respondent will take with respect to personal information it has collected in the event that it changes the terms of the privacy policy in effect at the time the information was collected;
- the extent to which the service allows parents to control what the information their children can provide to participating sites or the use of that information by such sites; and
- any other matter regarding the collection, use, or disclosure of personally identifiable information.

Part II of the proposed order requires Microsoft to establish and maintain a comprehensive information security program in writing that is reasonably designed to protect the security, confidentiality, and integrity of personal information collected from or about consumers. The security program must contain administrative, technical, and physical safeguards appropriate to Microsoft's size and complexity, the nature and scope of its activities, and the sensitivity of the personal information collected from or about consumers. Specifically, the order requires Microsoft to:

- designate an employee or employees to coordinate and be accountable for the information security program;
- identify material internal and external risks to the security, confidentiality, and integrity of customer information that could result in the unauthorized disclosure, misuse, alteration, destruction, or other compromise of such information, and assess the sufficiency of any safeguards in place to control these risks. At a minimum, this risk assessment will include consideration of risks in each area of relevant operation, including: (1) employee training and management; (2) information systems, including network

Analysis

and software design, information processing, storage, transmission and disposal; and (3) prevention, detection, and response to attacks, intrusions, or other systems failures.

- design and implement reasonable safeguards to control the risks identified through risk assessment, and regularly test or monitor the effectiveness of the safeguards' key controls, systems, and procedures.
- evaluate and adjust its information security program in light of the results of testing and monitoring, any material changes to its operations or business arrangements, or any other circumstances that Microsoft knows or has reason to know may have a material impact on its information security program.

Part III of the proposed order requires that Microsoft obtain within one year, and on a biannual basis thereafter, an assessment and report from a qualified, objective, independent third-party professional, using procedures and standards generally accepted in the profession, certifying that: (1) Microsoft has in place a security program that provides protections that meet or exceed the protections required by Part II of this order; and (2) Microsoft's security program is operating with sufficient effectiveness to provide reasonable assurance that the security, confidentiality, and integrity of consumer's personal information has been protected.

Parts IV through VII of the proposed order are reporting and compliance provisions. Part IV requires Microsoft's retention of materials relating to its privacy and security representations and to its compliance with the order's information security program. Part V requires dissemination of the order now and in the future to persons with responsibilities relating to the subject matter of the order. Part VI ensures notification to the FTC of changes in corporate status. Part VII mandates compliance reports within sixty (60) days after service of the order and at such other times as the Federal Trade Commission may require. Part VII is a

Analysis

provision "sunsetting" the order after twenty (20) years, with certain exceptions.

The purpose of this analysis is to facilitate public comment on the proposed order. It is not intended to constitute an official interpretation of the agreement and proposed order or to modify their terms in any way.