



Your Identity Theft Protection | FAQ



“ “ *IdentityForce is the best online identity monitoring service in the country!* ” ”

— *Deeana Johnson*

Verified Reviewer

Original review: August 13, 2020



PRODUCT & SERVICE OVERVIEW

Q: What services does IdentityForce offer?

A: NVIDIA recognizes the exponential increase in fraud and scams in 2020, and the vulnerabilities that result from having sensitive personal information exposed. Since partnering with IdentityForce in 2016, NVIDIA employees have benefited from world-class identity theft protection plans built to proactively monitor, alert, and help you fix any identity theft compromises. **You may select an UltraSecure Premium Individual or Family identity theft protection plan**, IdentityForce's most popular and comprehensive plan, at up to **60% off** retail pricing. IdentityForce's top-rated consumer ID theft protection plans will monitor your personal information and quickly notify you about any suspicious activity. If your identity is compromised, IdentityForce has your back. You'll get access to fraud experts and fully managed restoration services so that you don't need to worry about the paperwork, phone calls, and minutia that goes with restoring your good name. Combined with the \$1 million identity theft insurance coverage, you get a further layer of protection. You can also learn more [here](#).

ENROLLMENT & REGISTRATION

Q: How do I enroll in IdentityForce?

A: Upon election of the Individual or Family identity theft protection plan benefit through your NVIDIA benefit site, www.nvidiabenefits.bswift.com, you will receive a welcome email from IdentityForce with instructions to complete the registration process, setup your account, and activate your identity protection monitoring and alerts. **If you do not receive this email by the first of the month following your benefit election, please contact memberservices@identityforce.com, subject line "NVIDIA Welcome Email".**

Q: I am confused about completing my registration to activate my identity theft protection services. Who can help me?

A: Send an email to memberservices@identityforce.com with the subject "NVIDIA complete registration link" or call IdentityForce Member Services at (877) 694-3367.

Q: Best practice is not to click on a link in an email. How can I register without clicking on the link?

A: You can call IdentityForce Member Services at (877) 694-3367 and they will be able to register you.

Q: What is the least amount of information that I must provide to IdentityForce?

A: The minimum amount of information IdentityForce requires is first name, last name and email to activate your services so they are available to you when you need identity restoration services after an identity theft incident. However, we would encourage you to take the time to fully register and start benefiting immediately from all the monitoring and alert services IdentityForce provides. **Watch this [short tutorial](#) that can help you quickly navigate the three core things you should do upon signing up for IdentityForce.**



DEPENDENTS

Q: Are my dependents covered by IdentityForce?

A: Yes. As part of the identity protection plans being offered to NVIDIA's employees, **child identity theft protection is included with every individual and family plan** and will be activated once you have fully registered. Children are defined as dependents 25-years-old and under. Children receive a tailored identity protection product from IdentityForce named ChildWatch, which is available to protect all children in the household.

Q: How can I add my spouse or domestic partner to this service?

A: The identity protection benefit is available as a Family plan, which includes the NVIDIA employee and one additional adult, plus unlimited children within the household. Once you have enrolled and activated your Family plan you will be able to add an additional adult from your IdentityForce account. Remember, children are enrolled in ChildWatch at no additional cost for individual plans and family plans.

VICTIMS OF IDENTITY THEFT

Q: How does IdentityForce help me recover from identity theft?

A: IdentityForce plans include best-in-class [Restoration Services](#), where you'll gain access to Certified Protection Experts who offer comprehensive, 24/7 recovery services. Your dedicated specialist will complete paperwork, make calls, and handle every detail to restore your identity. All IdentityForce plans also include **White-glove Family Restoration**, which provides recovery services for your household family members in the event of identity theft. This includes parents, siblings, and children of the primary account holder.

Q: What if I become a victim of identity theft, but I haven't completed my registration?

A: If you have already elected the IdentityForce identity theft protection plan benefit, but have not completed your registration, you are still entitled to fully managed restoration and you also benefit from the \$1M identity theft insurance. If you become a victim of an identity crime, we highly recommend completing your IdentityForce registration to activate all your identity monitoring services. Watch [a short tutorial video here](#) that will help you navigate quickly to having control over your privacy and security with IdentityForce.

Q: I'm a victim of identity theft. Does IdentityForce help me to restore my identity after the theft has been identified?

A: Yes, you will receive fully managed restoration services from a dedicated Identity Restoration Specialist in the event of an identity theft incident, including preexisting conditions. The \$1M identity theft insurance policy does not apply to preexisting conditions, but all other restoration services are included.

Q: Does the \$1M guarantee apply to any loss incurred as a result of me being breached?

A: Your ID theft protection includes a \$1M identity theft insurance policy, covering certain out-of-pocket costs and lost funds as a result of an identity theft incident. A complete copy of the insurance policy is available through IdentityForce Member Services at (877) 694-3367.

ALERTS

Q: When I provide my bank login credentials for Bank and Credit Card Activity Alerts, does that violate my credit card terms and conditions?

A: To ensure compliance, we encourage you to review each cardholder agreement carefully. You can also contact your bank or credit card issuer for more information about their policies. Your identity theft protection benefit includes many features including advanced fraud monitoring, credit report monitoring and \$1M identity theft insurance, even if you do not use the Bank and Credit Card Activity alerts.

Q: How can I limit the number of bank and credit card activity alerts?

A: There are several ways to reduce the number of alerts sent from IdentityForce's Bank and Credit Card Activity alerts service.

1. The service sends alerts based on four types of transactions [purchases, withdrawals, transfers, and duplicates] – each can be turned on or off individually under Alert Preferences when you log in to your IdentityForce account.
2. A member can also set limits for each type of transaction [i.e. Alert me if a purchase is over \$300]. To reduce the number of alerts, raise the alert setting [i.e. Alert me if a purchase if over \$500 or \$1000, etc.]

Q: Why do some requests require a state identification?

A: Websites that list people's public records require the person requesting a change to provide a copy of their State ID to confirm that the requester possesses an ID. When uploading your ID, we recommend blacking out your photo and ID number.

Q: How does IdentityForce obtain my information from people search sites?

A: IdentityForce uses custom technology code to scan people search sites for a member's personal information and creates a report of what information is found and where.

Q: Can I disable the Sex Offender Alerts?

A: NVIDIA is offering IdentityForce UltraSecure Premium as an opt-in benefit to all its employees. IdentityForce's UltraSecure is a commercially available product with a large consumer base who finds meaningful value in the sex offender alert feature, and it is not an optional alert. One of the most important aspects of this protection is that it notifies a member if a sex offender fraudulently registers using the member's identity. It also shows the location of registered sex offenders in a defined area based on the member's zip code which is public record.

CREDIT MONITORING

Q: How often can I request my credit score?

A: With UltraSecure Premium protection, you have access to your VantageScore® 3.0 credit score, updated monthly. This credit score is based on data from the three national credit bureaus, TransUnion, Experian, and Equifax. Your plan also includes Credit Score Tracker, which monitors credit scores over time with a month-after-month graph.

Q: How is IdentityForce's credit reporting different from other credit reporting agencies?

A: IdentityForce's UltraSecure Premium plan provides you with a quarterly credit report that merges the data from all three national bureaus to give you a detailed report of your credit history with instant online access. You can spot fraud quickly with daily monitoring of your credit report and alerts if key changes are detected.

ADDITIONAL PROTECTION BENEFITS

Q: How does IdentityForce protect me from COVID-19 scams and fraud?

A: From Dark Web Monitoring and Bank Activity Alerts, to Online PC Protection Tools and Social Media Identity Monitoring, IdentityForce protects you against the exponential increase in scam and fraud activity that has occurred since the pandemic. You can learn more about these key capabilities that continuously work to protect you [here](#).

Q: How does IdentityForce protect me from mobile threats?

A: Every IdentityForce member can download the IdentityForce mobile app for Android and Apple iOS devices. The app features Mobile Attack Control, a comprehensive mobile device scan that delivers alerts for a wide array of threats, including rouge apps, spyware, unsecured Wi-Fi connections, and fake or “spoofed” networks. The mobile app also includes a secure Virtual Private Network (VPN), that provides a secure internet connection anywhere you go. Read more about IdentityForce mobile threat protection [here](#).

Q: What educational materials does IdentityForce provide?

A: Your membership gives you access to breach and scam news, actionable tips, and sharable infographics, all designed to help you protect what matters most. Your IdentityForce member dashboard includes the latest articles, along with tools to assist with junk mail opt-out, placing credit freezes, and credit report fraud assistance, among many other useful identity protection resources.

CHANGES AND CANCELLATIONS

Q: Can I change or cancel my IdentityForce coverage at any time?

A: Yes, your IdentityForce membership is a voluntary benefit offered by NVIDIA. To change or cancel your coverage, please visit the [NVIDIA Benefits Enrollment Portal \(www.nvidiabenefits.bswift.com\)](http://www.nvidiabenefits.bswift.com), under life event, select “Add/drop identity theft coverage”.

If your NVIDIA employment ends, and you do not wish to continue your membership through direct billing with IdentityForce, you may request to have your personal information removed from the IdentityForce system. Contact IdentityForce Member Services at (877) 694-3367.

DATA PROTECTION

Q: How does IdentityForce protect the information provided by its members?

A: IdentityForce, a Sontiq brand, is committed to following global data privacy standards and practices, including helping members understand their rights and responsibilities. Learn more at [Sontiq's Trust Center](#). IdentityForce operates a risk-based information systems security management program that implements industry-standard best practices for protecting member data. IdentityForce meets or exceeds the superset of the requirements of these standards and regulations: Payment Card Industry (PCI) Level 1; SSAE-16 SOC2 Level II; NIST 800-53 R4 at the High security categorization, including the privacy controls; State privacy regulations, such as the California Consumer Protection Act (CCPA); EU-US Data Privacy Shield Privacy Policy; EU GDPR (European Union General Data Protection Plan). Sontiq security is independently audited to ensure that it meets industry standards of security, including the Payment Card Industry (PCI) Data Security Standard (DSS), SSAE16 (Statement on Standards for Attestation Engagements 16) Statement of Compliance (SOC2) and NIST 800-53 R4.

Q: Once a member cancels, what happens to the member's personal information?

A: If a member's account is canceled due to employment termination, the IdentityForce system retains information necessary to facilitate reinstatement of the member's account. The member may request to have their information purged from the IdentityForce system, in accordance with the global data privacy standards and practices adhered to by Sontiq. Learn more at [Sontiq's Trust Center](#). Please contact Member Services at (877) 694-3367.

Q: How am I protected if IdentityForce's systems are breached?

A: In the event IdentityForce experiences a data breach during the term of our contract that affects NVIDIA employees, all members are covered by \$1M identity theft insurance policy and entitled to fully managed restoration services.

ABOUT SONTIQ

Sontiq is a high-tech security and identity protection company arming businesses and consumers with award-winning products built to protect what matters most. Sontiq's brands, [EZShield](#) and [IdentityForce](#), provide a full range of identity monitoring, restoration, and response products and services that empower customers to be less vulnerable to the financial and emotional consequences of identity theft and cybercrimes. Learn more at www.sontiq.com or engage with us on [Twitter](#), [Facebook](#), [LinkedIn](#), or [YouTube](#).

