

Stolen Identity Event Group Insurance

Summary of Coverage

This Master Policy is registered and delivered as a surplus lines coverage under the Insurance Code of Washington, title 48 RCW. It is not protected by any Washington State guaranty association law. The broker that procured the Master Policy is Marsh USA LLC, 12421 Meredith Drive, Ste 300, Urbandale, IA 50323.

This Summary of Benefits document provides only a summary of the benefits entitled to you as a customer of Gen Digital Inc., the policyholder of a group policy (“the policy”). Based on the specific service package you are enrolled in, benefits may vary, as outlined below. **This is a summary only. Additional terms and conditions apply.** A copy of the policy will be made available upon request. Refer to the full policy for all terms, conditions, and exclusions. Your entitlement to benefits under the group policy will terminate upon termination of your enrollment in any **Insured Program**.

Schedule

Insuring Company

Name	HSB Specialty Insurance Company
Mailing Address	One State Street, P.O. Box 5024, Hartford, Connecticut 06102-5024

Provider Details

Provider	Gen Digital Inc.
Mailing Address	60 E Rio Salado Parkway, Suite 1000, Tempe, Arizona, 85281

Insured Programs

Insured Program Name	Genie Scam Protection Pro
Coverage Type	Individual
Coverage Aggregate Limits	
Cyber Extortion	\$10,000
Online Fraud Reimbursement	\$10,000

Online Scams	\$10,000
<u>Member Details</u>	
Member Annual Aggregate Limit	\$10,000
Member Deductible	\$100 <i>per occurrence</i>

The words “we”, “us” and “our” refer to the Insuring Company shown in the Schedule of this Summary of Benefits.

Titles given to paragraphs throughout this Summary of Benefits are for assistance in finding applicable provisions.

Titles do not grant, define or restrict coverage.

A. DEFINITIONS

1. **Computing device** means a desktop, laptop or tablet computer or Wi-Fi router or other internet access point.
Such device must be owned or leased by a **member**, as well as operated under the **member's** control.
2. Connected home device means any electronic device, other than a **computing device**, that connects to the internet or to other electronic devices. This includes, but is not limited to, networked versions of any of the following:
 - a. Smart phones;
 - b. Thermostats;
 - c. Entertainment systems;
 - d. Appliances;
 - e. Smoke, fire and home security monitoring systems; or
 - f. Cameras.
 Such device must be owned or leased by a **member**, as well as operated under the **member's** control.
3. **Cyber extortion event** means one of the following involving a **computing device** or **connected home device**:
 - a. A demand for money or other consideration based on a credible threat to damage, disable, deny access to or disseminate content from a **member's** device,

system or data; or

b. A demand for money or other consideration based on an offer to restore access or functionality in connection with an attack on a **member's** device, system or data.

4. **Cyber extortion response costs** means any payment made as directed in response to a **cyber extortion event**, but only when that payment is:
 - a. Incurred as a direct result of a **cyber extortion event** directed against a member; and
 - b. Approved in advance by us. However, we may pay for **cyber extortion response costs** that were not approved in advance by us if we determine the following:
 - (1) It was not practical for the **member** to obtain our prior approval; and
 - (2) If consulted at the time, we would have approved the payment.
5. **Fraud costs** means the amount fraudulently taken from a **member**. This is the direct financial loss only. **Fraud costs** does not include any of the following:
 - a. Other expenses that arise from the **fraud event**;
 - b. Indirect loss, such as bodily injury, lost time, lost wages, identity recovery expenses or damaged reputation;
 - c. Any interest, time value or potential investment gain on the amount of financial loss; or
 - d. Any portion of such amount that has been or can reasonably be expected to be reimbursed by a third party, such as a financial institution.
6. **Fraud event**
 - a. **Fraud event** means any of the following, when such event is wholly or partially perpetrated through a **computing device** or **connected home device** and results in direct financial loss to a **member**:
 - (1) An **identity theft event**;
 - (2) The unauthorized use of a card, card number or account number associated with a bank account or credit account issued to or registered in a member's name, when the member is legally liable for such use;
 - (3) The forgery or alteration of any check or negotiable instrument;
 - (4) Acceptance in good faith of counterfeit currency; or
 - (5) **Online scams**.
 - b. **Fraud event** does not mean or include any occurrence:
 - (1) In which a **member** is threatened or coerced to part with something of value, other than online scams;
 - (2) Between a **member** and any of the following:
 - (a) Any other **member**;

(b) A **member's** current or former spouse, common law spouse or domestic partner; or

(c) A **member's** grandparent, parent, sibling, child or grandchild.

(3) Involving use of a card, card number or account number associated with a bank account or credit account:

(a) By a person who has ever received any authorization from a **member** to use such card, card number or account number; or

(b) If a **member** has not complied with all terms and conditions under which such card, card number or account number was issued.

(4) Arising from any of the following:

(a) The business or professional service of a **member**.

(b) A dispute or a disagreement over the completeness, authenticity or value of a product, a service or a financial instrument.

(c) A gift or charitable contribution to an individual or any legitimate organization.

(d) An online auction or the use of an online auction site.

(e) A lottery, gambling or a game of chance.

(f) An advance fee fraud or other fraud in which a **member** provides money based on an expectation of receiving at some future time a larger amount of money or something with a greater value than the money provided.

7. **Identity theft event** means the fraudulent use of social security number or other **personally identifying information**. This includes fraudulently using such information to establish credit accounts, secure loans, enter into contracts or commit crimes.

8. **Insured program** means the package of products and/or services provided by the **provider** and shown under the Insured Programs section of the Schedule of this Summary of Benefits.

9. **Member** means:

a. The **primary member**.

b. If the **insured program** includes coverage for family members, the residents of the household of the **primary member** who are:

(1) The relatives of such persons, including their spouse; or

(2) Under the age of 21 and in the care of such persons; or

(3) A student enrolled in school full-time, as defined by the school, who was a resident of the **primary member's** household before moving out to attend school, provided the student is under the age of:

(a) 24 and the **primary member's** relative; or

(b) 21 and in the primary member's care or the care of a resident of the **primary member's** household who is the **primary member's** relative.

10. **Nuclear Hazard** means nuclear reaction, radiation or radioactive contamination, or any consequence of any of these, however caused and whether controlled or uncontrolled.
11. **Occurrence** means all **stolen identity events**, **cyber extortion events**, or **fraud events** that:
 - a. Occur at the same time; or
 - b. Arise during the same policy period from the same source, cause or vulnerability
12. **Online scams** means intentional and criminal deception of a **member**, perpetrated partially or wholly through a **computing device** or **connected home device**, to induce the **member** to:
 - a. Disclose login credentials that results in a financial loss of money, securities, cryptocurrency or tangible property; or
 - b. Part voluntarily with money, securities, cryptocurrency or tangible property.
13. **Personally identifying information**
 - a. **Personally identifying information** means information, including health information, that could be used to commit fraud or other illegal activity involving the credit, access to health care or identity of a member. This includes, but is not limited to, Social Security numbers, account numbers, passwords or login credentials, or other methods to access or control a **computing device** or **connected home device** system identification.
 - b. **Personally identifying information** does not mean or include information that is otherwise available to the public, such as names and addresses.
14. **Primary member** means a person who, at the time of the discovery of the **stolen identity event**, is a customer in good standing of the **provider** and is directly enrolled in the **insured program**.
15. **Provider** means the entity providing the **insured program** and shown as the Provider in the Schedule of this Summary of Benefits.
16. **Stolen identity event** means the theft, accidental release, publication or misappropriation of a **member's personally identifying information** that results in or could reasonably result in the wrongful use of the information. This includes a **cyber extortion event** or **fraud event**, but only to the extent that such corresponding coverages are included in the **insured program**.

B. COVERAGE

1. COVERAGE REQUIREMENTS

This Stolen Identity Event Group Insurance applies only if all of the following conditions are met:

- a. There has been a **stolen identity event** involving the **personally identifying information** of a **member**; and
- b. Such **stolen identity event** is first discovered by the **member** during the policy period for which the policy is applicable; and
- c. Such **stolen identity event** is reported to us as soon as practicable, but in no event more than 60 days after the date it is first discovered by the **member**.

2. COVERAGES PROVIDED

If all of the conditions listed above in 1. **COVERAGE REQUIREMENTS** have been met, then we will provide the **member** the following coverages for loss directly arising from such **stolen identity event**.

a. Cyber Extortion

If there has been a **cyber extortion event** as a direct result of such **stolen identity event**, then we will provide the **member** the following coverages for loss directly arising from such **cyber extortion event**:

- (1) Professional assistance from a subject matter expert provided by us for advice and consultation regarding how best to respond to the threat.
- (2) Reimbursement of the **member's** necessary and reasonable **cyber extortion response costs**.

b. Online Fraud Reimbursement

If there has been a **fraud event** that is wholly or partially perpetrated through a **computing device** or **connected home device** as a direct result of such **stolen identity event**, then we will pay the **member's** necessary and reasonable **fraud costs**.

C. EXCLUSIONS

The following exclusions apply to all coverages under the policy.

We will not pay for loss, damage or expense caused by or resulting from:

1. Any of the following by a **member**:
 - a. Criminal, fraudulent or dishonest acts, errors or omissions;
 - b. Intentional violations of the law; or
 - c. Intentionally initiating or contributing to a covered loss event.
2. Any criminal investigations or proceedings.

3. Any physical damage or bodily injury.
4. Any third party liability or legal defense costs.
5. Any damage to a motor vehicle, watercraft, aircraft or other vehicle.
6. Any fines or penalties.
7. Damage to any device or system that is not owned or leased by a **member**, or operated under the **member's** control or the control of another **member**.
8. Loss arising from any business, including but not limited to any business owned or operated by any **member** or any business employing any **member**.
9. Costs to research or correct any deficiency.
10. Any **stolen identity event** first discovered by a **member** prior to the inception of the **member's** coverage under the policy.
11. Any **stolen identity event** first occurring more than 60 days prior to the inception of the **member's** coverage under the policy.
12. Any costs or expenses associated with a **stolen identity event** if such costs or expenses are incurred more than one year from the expiration date of the policy.
13. Any **nuclear hazard**.
14. Any governmental action, meaning the destruction, confiscation or seizure of property by order of any governmental or public authority.
15. War, including the following and any consequence of any of the following:
 - a. Cyber warfare, whether or not occurring in combination with physical combat;
 - b. Undeclared war;
 - c. Civil war;
 - d. Hostile action by military force or cyber measures, including action in defending against or hindering an expected or actual attack, by any Combatant; or
 - e. Insurrection, rebellion, revolution, usurped power, political violence or action taken by governmental authority in defending against or hindering any of these, including cyber action in connection with any of the foregoing.For purposes of this exclusion, cyber warfare, cyber measures and cyber action include, but are not limited to, the use of disruptive digital activities against a computer network or system with the intention to cause harm in order to further political or similar objectives, or to intimidate any person(s) in furtherance of such objectives, committed by a Combatant.

The attribution of an action to a Combatant will be determined by relying on reasonable evidence such as:

- a. Statements by an impacted government, sovereign or other authority;
- b. Statements by widely recognized international bodies (such as the United Nations) or alliances (such as the North Atlantic Treaty Organization); or
- c. Consensus opinion within relevant expert communities such as the cyber security industry. Decisions about the presence or absence of war, hostile action, and other terms used in this exclusion will take into consideration the full range of available tactics, weapons and technologies at the time of the event giving rise to the loss.

Combatant means, for purposes of this exclusion, a government, sovereign or other authority, or agents acting on their behalf.

- 16. Total or partial failure or interruption of, reduction in performance of, or damage to any electrical power supply network or telecommunication network not owned and operated by a **member** including, but not limited to, the internet, internet service providers, Domain Name System (DNS) service providers, cable and wireless providers, internet exchange providers, search engine providers, internet protocol networks (and similar networks that may have different designations) and other providers of telecommunications or internet infrastructure.
- 17. Any loss resulting directly or indirectly from any errors or omissions by a **member** or a financial institution in the input or processing of data.
- 18. Any loss related to the financial performance of any investments.
- 19. Any loss occurring while the **primary member** is not an active customer in good standing of the **provider** and directly enrolled in the **insured program**.
- 20. Any **member** whose primary residence is located in New York or Washington state.
- 21. Any loss claimed by the **provider**.
- 22. Any amount not insurable under applicable law.
- 23. Any provision of coverage under the policy to the extent that such provision would expose the **member** or **provider** to a violation of economic or trade sanctions, laws or regulations of the United States of America or any other jurisdiction with whose laws we are legally obligated to comply.

D. LIMITS

The Member Annual Aggregate Limit shown in the Schedule of this Summary of Benefits under the applicable **insured program** is the most we will pay for all loss, damage or

expense for any one **member** arising during any one policy period for all coverages provided by the policy. If the **insured program** includes coverage for family members, then the Member Annual Aggregate Limit is the most we will pay for all loss, damage or expense for all **members** associated with any one **primary member** for all coverages provided by the policy. This limit shall apply to the total of all loss, damage or expense arising from all **stolen identity events** discovered during such policy period.

The Coverage Aggregate Limit for each coverage shown in the Schedule of this Summary of Benefits under the applicable **insured program** is the most we will pay for all loss, damage or expense for any one **member** arising during any one policy period for such coverage. If the **insured program** includes coverage for family members, then the Coverage Aggregate Limit is the most we will pay for all loss, damage or expense for all members associated with any one **primary member** for such coverage. This limit shall apply to the total of all loss, damage or expense arising from all **stolen identity events** discovered during such policy period.

If any **occurrence** causes loss, damage or expense in more than one policy period, all such loss, damage and expense will be subject to the Member Annual Aggregate Limit of the first policy period in which the occurrence was discovered.

Fraud costs resulting from Item a.(5). (**online scams**) of the definition of **fraud event** is subject to the sublimit shown in the Schedule of this Summary of Benefits. This sublimit is part of, and not in addition to, the Online Fraud Reimbursement Coverage Limit.

E. DEDUCTIBLE

We will pay only that part of the total payable loss that exceeds the sum of the Member Deductible shown in the Schedule of this Summary of Benefits under the applicable **insured program**, subject to the applicable limits shown in the Schedule of this Summary of Benefits. **The member** will be responsible for the applicable Member Deductible under the applicable **insured program**, if shown in the Schedule of this Summary of Benefits.

F. CONDITIONS

The following conditions apply to all coverages under the policy:

1. Assignment

Assignment of the policy will not be valid unless we give our written consent.

2. Bankruptcy

Our obligations under the policy will not be relieved by the bankruptcy or insolvency of a **member** or **provider**.

3. Cancellation/Termination

a. The **provider** may cancel the policy with 120 day notice by informing us in writing of the date cancellation is to take effect.

b. We may cancel the policy only for the reasons stated below by informing the **provider** in writing of the date cancellation takes effect. This cancellation notice may be delivered to the **provider**, or mailed to the **provider** at their mailing address shown in the Declarations of the policy. Proof of mailing will be sufficient proof of notice.

(1) When the **provider** has not paid the premium, we may cancel at any time by letting the **provider** know at least 30 days prior to the date cancellation takes effect.

(2) When the policy has been in effect for less than 60 days and is not a renewal with us, we may cancel for any reason by letting the **provider** know at least 10 days prior to the date cancellation takes effect.

(3) When the policy is a renewal with us or has been in effect for 60 days or more, we may cancel:

(i) If there has been a material misrepresentation which if known to us would have caused us not to issue the policy; or

(ii) If the risk has changed substantially since the policy was issued.

This can be done by letting the **provider** know at least 30 days before the date cancellation takes effect.

(4) When the policy is written for a period of more than one year, we may cancel for any reason at anniversary by letting the **provider** know at least 120 days before the cancellation takes effect.

c. When the policy is cancelled, the premium for the period from the date of cancellation to the expiration date will be refunded pro rata.

d. If the return premium is not refunded with the notice of cancellation or when the policy is returned to us, we will refund it within a reasonable time after the date cancellation takes effect.

e. The **provider** is responsible for informing **members** of a non-renewal or cancellation of the policy.

f. **Member** coverage under the policy shall terminate upon the termination of the **primary member's** enrollment in the **insured program** or the termination of the policy, in accordance with the terms of the policy, whichever is earlier.

4. Changes

The policy contains all the agreements between the **provider** and us concerning the insurance afforded. The **provider** shown in the Schedule of this Summary of Benefits is authorized to make changes in the terms of the policy with our consent.

The policy's terms can be waived or amended only by endorsement issued by us and made a part of the policy. The **provider** is responsible for informing **members** of any changes to the policy.

5. **Concealment or Fraud**

We do not provide coverage to a **member** who, whether before or after a loss, has:

- a. Intentionally concealed or misrepresented any material fact or circumstance;
- b. Engaged in fraudulent conduct; or
- c. Made false statements;

relating to this insurance.

6. **Confidentiality**

With respect to Cyber Extortion coverage, **members** must make every reasonable effort to avoid divulging the existence of this coverage.

7. **Due Diligence**

Members must agree to use due diligence to prevent and mitigate costs covered under the policy. This includes, but is not limited to, complying with reasonable and widely-practiced steps for:

- a. Providing and maintaining appropriate system and data security; and
- b. Maintaining and updating at appropriate intervals backups of electronic data.

8. **Duties After Loss**

In case of a loss, the following duties must be performed either by the **member** or the **member's** representative. If failure to comply with these duties is prejudicial to us, we have no duty to provide coverage under the policy:

- a. Give prompt notice to us;
- b. Notify the police if there has been a violation of the law;
- c. Notify the bank, credit card or electronic fund transfer card or access device company in case of a **fraud event** involving a bank card, credit card or check;
- d. Cooperate with us in the investigation or settlement as follows:
 - (1) Provide the following information within 30 days after our request:
 - (i) A description of how, when and where the **stolen identity event** occurred.
 - (ii) Written reports of any service providers who participated in the investigation of or response to the **stolen identity event**.
 - (iii) Written reports or correspondence to or from law enforcement or any governmental authority or agency, or similar organization.
 - (iv) Any additional information we request relevant to the investigation of the **stolen identity event**.

(2) As may be reasonably required, permit us or a third party appointed by us to inspect and audit the **computing device, connected home device**, and any records. Any additional expenses related to this Condition F.9.d.(2) will be paid by us and will be in addition to, and not part of, the Member Annual Aggregate Limit. We must approve such expenses in advance.

(3) Send us signed, sworn proof of loss that contains the information we request to investigate the **stolen identity event**. This must be done within 60 days after our request. We will supply the necessary forms.

9. **Legal Advice**

We are not the **members'** or **provider's** legal advisor. Our determination of what is or is not insured under the policy does not represent advice or counsel from us about what a **member** should or should not do.

10. **Nonrenewal**

We may elect not to renew the policy. We may do so by delivering to the provider, or mailing to the provider at their mailing address shown in the Declarations of the policy, written notice at least 120 days before the expiration date of the policy. Proof of mailing will be sufficient proof of notice.

11. **Other Insurance**

We shall be excess over any other insurance (including, without limitation, cyber insurance), product warranty, extended services agreement or contract. The policy is specifically excess of any cyber insurance policy carried by the **member**, in addition to any other insurance carried by the **member** that applies to a loss under the policy.

12. **Premium**

a. The premium shown in the Declarations of the policy was computed based on rates in effect at the time the policy was issued. Other than documented and verifiable change in applicable insurance premium taxes or legal or regulatory requirements requiring a change in the rates, we will only modify rates on the renewal effective date of the policy.

b. Premium will be calculated in accordance with the reporting and the rates shown in the Declarations of the policy, prorated based on the Reporting Period shown in the Declarations. A premium invoice will be issued to the **provider** within ten (10) business days of receipt of such reporting.

13. **Services**

a. We will only pay under the policy for services that are provided by service

providers approved by us. **Members** must obtain our prior approval for any service provider whose expenses they want covered under the policy. We will not unreasonably withhold such approval.

b. **Members** will have a direct relationship with service providers paid for in whole or in part under the policy. Those firms work for the **members**.

c. With respect to any services provided by any service provider paid for in whole or in part under the policy:

(1) The effectiveness of such services depends on **members'** cooperation and assistance.

(2) We do not warrant or guarantee that services will be available or applicable to all individuals. Service in Canada will be different from service in the United States and Puerto Rico.

(3) We do not warrant or guarantee that the services will end or eliminate all problems associated with the covered events.

14. Suit Against Us

No action can be brought against us unless there has been full compliance with all of the terms and conditions of the policy and the action is started within two years after the date of loss.

15. Transfer of Rights of Recovery Against Others to Us

If any member for whom we make payment under the policy has rights to recover damages from another, those rights are transferred to us to the extent of our payment. The **member** must do everything necessary to secure our rights and must do nothing after loss to impair them.

16. Venue and Choice of Law

Any dispute arising out of or related to the policy, or with respect to the application of or the interpretation of the policy, shall be governed by the laws of the state of Arizona, without giving effect to the principles of conflict of laws.

17. Waiver or Change of Policy Provisions

A change or waiver of a provision of the policy must be in writing by us to be valid. Our request for an appraisal or examination will not waive any of our rights.