## Sprint Security Support Services for Schedule No. 11*

Sprint Security Support Services are designed to minimize the vulnerability of Sprint's voice services customers to certain outbound international and inbound domestic toll free communications fraud originating from or terminating at the customer's enterprise telephone equipment.

### 1. Definitions

The following definitions apply to all Sprint Security Support Services.

1. Covered Domestic Toll Free Inbound Services

   Covered Domestic Toll Free Inbound Services includes all Sprint domestic toll free inbound services (excluding North American Dialing Plan locations in Canada, Mexico and the Caribbean).

2. Covered Outbound International Services

   Covered Outbound International Services include all Sprint long distance services from a customer's domestic CPE to international locations including Caribbean locations included in the North American Dialing Plan, excluding Canada and Mexico.

3. CPE (Customer Premises Equipment)

   CPE is a single PBX, a single electronic key system or a specific customer location supported by a Centrex system, with or without adjuncts such as voice mail and auto-attendants. CPE must be located in an area where usage recording, including originating number identification, is performed by Sprint within the United States, Puerto Rico and the U.S. Virgin Islands.

4. Sprint Notification

   Sprint Notification is the placement of a telephone call by Sprint to a telephone number currently in service for the customer or any employee/agent of the customer. Communication to the customer or an employee/agent of the customer via voice mail or fax also constitutes Sprint Notification.

5. Customer Notification

   Customer Notification is an answered telephone call made by the customer to the Sprint Security Support Service Unit to provide notice of suspected Remote Toll Fraud.

6. Remote Toll Fraud

   Remote Toll Fraud is an unauthorized call using (1) Covered Outbound International Services made by remotely accessing Customer’s CPE from another domestic location, breaching the security of that CPE or (2) Covered Domestic Toll Free Inbound Services that access a Customer’s CPE from another domestic location. In either case, calls made by, or in collusion with, students, faculty, persons employed or previously employed by the customer or agents of the customer are not considered Remote Toll Fraud.

7. Remote Toll Fraud Usage Charges

   Remote Toll Fraud Usage Charges are Sprint schedule charges for Remote Toll Fraud for which the breach of security occurred at a customer's CPE. Billing credits for Remote Toll Fraud Usage Charges are limited to actual telecommunications service usage.

* Sprint Security Support Services are no longer available for subscription.

## 1. Definitions (Continued)

8. Incident

An Incident is any previously undetected CPE fraud that is the subject of a Customer Notification or a Sprint Notification.

## 2. SprintGUARD Basic

SprintGUARD Basic is provided automatically to all Sprint business voice services customers at no charge. SprintGUARD Basic limits the customer's exposure for Covered International Outbound Services and Covered Domestic Toll Free Inbound Services for Remote Toll Fraud Usage Charges and provides for notification of suspected Remote Toll Fraud identified by Sprint or the customer.

1. Sprint Responsibilities

Sprint provides the following services to the customer through the SprintGUARD Basic Service:

- Daily account analysis.

- Sprint Notification of apparent abnormal account activity.

2. Customer Responsibilities

1. Security Requirements

During an investigation of an Incident or suspected Incident, Sprint reserves the right to obtain specific information from the customer regarding any password(s) used to remotely access the CPE. Any request for this information will come from a Sprint Security Support Services representative.

2. Administrative Requirements

The customer must cooperate fully with Sprint in all efforts to stop suspected or confirmed Remote Toll Fraud.

3. Post-Claim Requirements

The customer must give Sprint access to the affected CPE within 24 hours of Sprint's request and permit the Sprint Security Support Service Team to investigate the current and/or former configuration of the CPE. The Customer must permit Sprint Security Support Service representatives to enter and inspect any CPE location within 12 hours of the termination of suspected Remote Toll Fraud if requested as part of an investigation of suspected Remote Toll Fraud.

The customer must make a Customer Notification to the Sprint Security Support Service Unit to report a suspected Incident, regardless of which local or long distance carrier is involved, within 2 hours of discovering the suspected Incident. In the absence of an applicable Sprint Notification or a Customer Notification, the customer must review its Sprint bill and notify Sprint in writing within 60 days after the date of the bill to report a suspected Incident. Usage charges not identified to or by Sprint within the specified 60 day period do not qualify as Remote Toll Fraud Usage Charges. The customer must establish (e.g., by way of call detail records) that each usage charge identified qualifies as a Remote Toll Fraud usage charge.

* Sprint Security Support Services are no longer available for subscription.

**2. SprintGUARD Basic (Continued)**

2. Customer Responsibilities (Continued)

3. Post-Claim Requirements

The customer must notify the Sprint Security Support Service Unit in writing within 30 days of the termination of the Incident of the means by which the fraud occurred, if known, and the changes made to the CPE to stop the Incident.

Customer must cooperate with Sprint's Security Support Service Unit in any prosecution of individuals for fraud, including, but not limited to, providing witnesses when necessary and allowing Sprint to review any relevant documents within the possession of customer.

Failure to cooperate or comply with any of the provisions set forth above will automatically disqualify the customer for current and future credits for Remote Toll Fraud Usage Charges at all customer locations.

3. Customer Liability

Customers of SprintGUARD Basic will remain liable for the first $15,000 per Incident in Remote Toll Fraud Usage Charges for calls prior to a Sprint Notification or a Customer Notification. Sprint will credit customer's invoices for all Remote Toll Fraud Usage Charges in excess of $15,000 per Incident incurred before Sprint Notification or Customer Notification. Customers remain liable for all Remote Toll Fraud Usage Charges which are incurred after Sprint Notification or Customer Notification.

If a qualifying Incident (as described above) occurs, customer will not receive any further SprintGUARD billing credits for the CPE in question again, or any other CPE connected to the CPE in question, until a "30 day fraud-free period" has elapsed from the date of the last fraudulent call of the last Incident affecting that CPE.

3. **SprintGUARD Plus**

SprintGUARD Plus is a subscription-based service designed to limit the customer's financial exposure for Covered International Outbound Services and Covered Domestic Toll Free Inbound Services for Remote Toll Fraud Usage Charges to a greater extent than the coverage afforded under the SprintGUARD Basic plan.

1. Sprint Responsibilities

SprintGUARD Plus incorporates all the same Sprint services as those afforded under SprintGUARD Basic.

2. Customer Responsibilities

The Customer agrees to complete and comply with the following in order to qualify for SprintGUARD Plus coverage:

- Complete a Customer Profile, international calling frequency worksheet, and location summary of service for each CPE.

* Sprint Security Support Services are no longer available for subscription.

3. **SprintGUARD Plus (Continued)**

2. Customer Responsibilities (Continued)

- Provide all information requested by Sprint which in Sprint's opinion is relevant to assist in the identification and prevention of Remote Toll Fraud.
- Authorize and initiate Class of Service (COS) Screening to limit outbound international (011-) and Caribbean (809 and others) direct calling codes where no business requirement exists.
- At all covered locations:
- Use a minimum of 8 digits for each Direct Inward System Access (DISA) code.
- Disable all voice mail and auto attendant external call transfer capabilities.
- Disable all voice mail system capability to transfer or route traffic to the trunk level.
- Deactivate maintenance dial-up ports on all Covered Equipment or install a security system on all CPE remote maintenance ports, e.g., call back or alpha numeric password (minimum of 8 characters).
- Delete all CPE manufacturer or vendor installed default passwords.
- Provide the name, telephone and pager numbers of 3 employees or agents, 1 voice mail box telephone number and 1 fax telephone number, each of which can be reached 24 hours a day, 365 days a year.
- Within 2 hours of a suspected Incident, make a Customer Notification to the *SprintGUARD* Security Support Service Unit (1-800-826-1898), regardless of interexchange or local exchange carrier involved or magnitude of the suspected fraud.
- Notify Sprint Fraud Management, in writing, of any additions, deletions or changes of Covered Equipment, international and Caribbean calling patterns, and SprintGUARD CPE Customer Profile information required by this Service Agreement.
- Develop an action plan to be implemented in the event of an Incident.
- Pay a non-recurring initial activation charge and monthly recurring charges per CPE as set forth in this Schedule.

3. Sprint Actions During an Incident

If for any reason the Customer cannot be reached by Sprint's Security Support Service Unit when suspicious calling patterns are identified, Sprint has the authority and permission of the customer to block whatever Sprint telecommunications services necessary to eliminate or minimize losses to Sprint and the customer, and the customer will indemnify and hold Sprint harmless for any and all direct or indirect losses or damages suffered by the customer or third parties as a result of the blocking of the customer's Sprint telecommunications services.

* Sprint Security Support Services are no longer available for subscription.

3. **SprintGUARD Plus (Continued)**

4. Customer Liability

Customers of SprintGUARD Plus will remain liable for the first $7,000 per Incident in Remote Toll Fraud Usage Charges for calls prior to a Sprint Notification or a Customer Notification. Sprint will credit Customer’s invoices for all Remote Toll Fraud Usage Charges in excess of $7,000 per Incident incurred before Sprint or Customer Notification. Customers remain liable for all Remote Toll Fraud Usage Charges which are incurred after Sprint or Customer Notification.

If a qualifying Incident (as described above) occurs, Customer will not receive any further SprintGUARD billing credits for the CPE in question again, or any other CPE connected to the CPE in question, until a "30 day fraud-free period" has elapsed from the date of the last fraudulent call of the last Incident affecting that CPE.

4. **SprintGUARD Elite**

SprintGUARD Elite is a subscription-based service for Sprint business voice services customers designed to offer maximum protection against the Customer's financial exposure for Covered International Outbound Services and Covered Domestic Toll Free Inbound Services for Remote Toll Fraud Usage Charges.

1. Sprint’s Responsibilities

Sprint’s responsibilities are identical to those identified for SprintGUARD Plus services.

2. Customer’s Responsibilities

Customer’s responsibilities are identical to those identified for SprintGUARD Plus services.

3. Customer Liability

Customers of SprintGUARD Elite are not liable for any Remote Toll Fraud Usage Charges for calls during an Incident prior to a Sprint Notification or a Customer Notification. Sprint will credit customer’s invoices for all Remote Toll Fraud Usage Charges per Incident incurred before Sprint Notification or Customer Notification. Customers remain liable for all Remote Toll Fraud Usage Charges which are incurred after Sprint Notification or Customer Notification.

If a qualifying Incident occurs, Customer will not receive any further SprintGUARD billing credits for the CPE in question again, or any other CPE connected to the CPE in question, until a "7 day fraud-free period" has elapsed from the date of the last fraudulent call of the last Incident affecting that CPE.

* Sprint Security Support Services are no longer available for subscription.

5. **Sprint Security Support Services Exclusions and Limitations**

1. Billing Credits Not Applicable for Remote Toll Fraud

Billing credits for Remote Toll Fraud will not be applicable in the following situations:

- Traffic carried by any carrier other than Sprint.
- Remote Toll Fraud occurring prior to the execution of an applicable Service Agreement.
- Remote Toll Fraud which terminates on toll-free service at an international or Caribbean location(s)
- Outbound CPE Remote Toll Fraud which terminates within the United States.
- Remote Toll Fraud resulting from the use of 1010XXX, wireless calls, calls placed by means of an operator service, 0 – or 0 + for network access, toll-free/900 pay-per-call traffic, authorization codes, calling cards, debit cards or credit cards provided or issued by any company.
- Remote Toll Fraud associated with colleges and universities.
- Remote Toll Fraud which occurs two (2) hours or later after Sprint Notification to Customer or Customer Notification to Sprint of suspected fraud.
- Any Incident, after the third Incident from the same Covered Equipment location, in which Sprint provided billing credits for Remote Toll Fraud within the 12 months prior to the Incident.
- Remote Toll Fraud resulting from the improper installation of Covered Equipment, including but not limited to security software or systems.
- For SprintGUARD Plus and Elite, Remote Toll Fraud occurring from Customer equipment not identified in a *SprintGUARD*® CPE Customer Profile.
- Remote Toll Fraud resulting from the Customer's negligence or the negligence of its employees, former employees, agents, vendors and independent contractors.
- Remote Toll Fraud resulting from intentional acts of the Customer, its employees, former employees, agents, vendors and independent contractors.
- Acts of God or actions outside the reasonable control of Sprint.

2. SprintGUARD Services Availability

SprintGUARD Services are available only in the United States, Puerto Rico, and the U.S. Virgin Islands. SprintGuard service is not available in other U.S. territories, protectorates and former possessions.

* Sprint Security Support Services are no longer available for subscription.

5. **Sprint Security Support Services Exclusions and Limitations**

3. Remote Toll Fraud and CPE Exclusions

Remote Toll Fraud does not include any 1010XXX calls, calls placed by means of a switchboard or an operator service, 0- or 0+ for network access, toll free/900 pay-per-call traffic, authorization codes either issued or generated by the customer, calling cards or credit cards provided or issued by any company, or Remote Toll Fraud to include calls from within an college or university campus. Sprint Security Support Services are available only to Sprint's customers and will not be provided in support of the customers of any Sprint customer.

Sprint Security Support Service will not cover any Remote Toll Fraud Usage Charges resulting from the negligence or intentional acts of the Customer, its employees, former employees, agents, vendors or independent contractors.

Sprint Security Support Services do not cover CPE that is not owned or leased by the customer and under the direct control of the customer.

Remote Toll Fraud Usage Charges which are not the responsibility of the customer pursuant to this schedule shall not count as valid usage charges for the purpose of determining any of the Customer's applicable volume/term discounts or for the purpose of satisfying any of the Customer's applicable volume/revenue commitments.

4. Limitations

To the extent that Sprint reduces or otherwise does not collect any Remote Toll Fraud Usage Charges for which the customer would have been liable if Sprint had not provided SprintGUARD services, Sprint shall be subrogated to any and all rights of the customer with respect to any associated claims against third parties (including, without limitations, any persons who facilitated or who made the unauthorized calls which constituted the Remote Toll Fraud).

**6.** **Sprint Security Support Services Charges**

1. SprintGUARD Basic

SprintGUARD Basic is provided automatically to all Sprint business voice services customers at no charge

2. SprintGUARD Plus

The following charges apply to SprintGUARD Plus service:

| Charges | Per Covered CPE |
|---|---|
| Non-Recurring Charges | |
| First 1000 covered CPEs | $50.00 |
| Additional CPEs over 1000 | Waived |
| Monthly Recurring Charges | |
| First 500 covered CPEs | $10.00 |
| Covered CPEs over 500 | Waived |

* Sprint Security Support Services are no longer available for subscription.

## 6. Sprint Security Support Services Charges (Continued)

### 3. SprintGUARD ELITE

The following charges apply to SprintGUARD Elite service:

| Charges | Per Covered CPE |
|---|---|
| Non-Recurring Charges | |
| First 100 covered CPEs | $200.00 |
| Additional CPEs over 100 | Waived |
| Monthly Recurring Charges | |
| First 100 covered CPEs | $150.00 |
| 101 - 200 CPEs | $100.00 |
| Each additional CPEs over 300 | $50.00 |

* Sprint Security Support Services are no longer available for subscription.