

Deutsche Telekom North America, Inc. Customer Proprietary Network Information Instructional Manual

I. PURPOSE

All employees already should have received and reviewed the **Customer Proprietary Network Information Protection Policy** (“CPNI Protection Policy”), which is located in your Employee Handbook. If you have misplaced your Employee Handbook, please contact **Human Resources**. This Manual applies only to Deutsche Telekom North America, Inc. T-Systems North America, Inc. has implemented its own CPNI manual. The purpose of this document is to explain how to implement that policy. In particular, this document addresses the following topics:

- The process for verifying a customer’s identity;
- What information can be disclosed to the customer upon customer request;
- What account modifications may be made by the customer upon customer request;
- When Deutsche Telekom North America, Inc. (“DTNA”) employees may use CPNI for marketing purposes;
- What to do if a DTNA employee receives a request for CPNI from law enforcement or any person other than the customer; and
- What to do if a DTNA employee learns of or suspects a breach of a customer’s CPNI.

These procedures are designed to protect DTNA and its customers. Recently, telecommunications companies have become victims of pretexters – persons pretending to be a customer in order to obtain that customer’s call detail records. These procedures are designed to prevent anyone other than the customer from gaining access to a customer’s account. If you have any concern that the person you are speaking with is not who he or she purports to be, please contact David Friedman at (212) 301-6014; do not release any information to the caller or make any changes to the purported customer’s account.

Our customers’ privacy is extremely important to us. DTNA employees are prohibited from using, sharing, or disclosing CPNI except as specified in the CPNI Protection Policy and this Manual. If you have any questions about the CPNI Protection Policy or this Manual, please contact David Friedman at (212) 301-6014.

Failure to comply with these procedures is grounds for disciplinary action, including potential termination.

II. VERIFICATION

DTNA personnel must verify a caller's identity on all incoming calls. Please record all information about the call in the customer service log.

Verification Procedures for Sales and Customer Support Personnel

The verification procedures in this section apply to DTNA Sales and Customer Support Personnel. For purposes of this manual, the term "Sales and Customer Support Personnel" includes Sales Managers, Sales Traders, Sales Support, and Credit and Collections personnel for both voice and non-voice products. Sales and Customer Support Personnel do *not* include Technical Support personnel.

- Assigned Sales Trader or Voice Trader: Each DTNA customer has an assigned Sales Trader or Voice Trader (as applicable). The assigned Sales Trader or Voice Trader generally will be the customer's first point of contact for sales and non-technical service related inquiries. If the assigned Sales Trader is unavailable, the available Sales Traders are permitted to assist the non-voice customers with inquiries unless otherwise stated herein or limited in the DTNA-customer contract. Similarly, if the assigned Voice Trader is unavailable, the available Voice Traders may assist the voice customers with inquiries
- Customer Contact Information: Each customer has designated a point(s) of contact with authority to act on the customer's behalf. The customer has the option of defining the authority for each designated point of contact (*e.g.*, a point of contact to handle service-related inquiries, a different point of contact to handle sales-related inquiries, etc.). For non-voice customers, the customer's designated points of contact and contact information are identified in each customer's contract. For all voice customers, the customer's designated account representatives and contact information are contained in the "Customer Pricing Requirements" spreadsheet.
- Inquiries Via Incoming Telephone Calls: The caller's identity must be verified on all incoming calls.
 - Upon receipt of an incoming call, please obtain the caller's name, company name, and account number.
 - If the caller is able to provide all of the requested information, please ask the caller for the purpose of the call. Please confirm that the caller is authorized to speak on behalf of the company for that purpose (*e.g.*, the customer has the authority to address billing inquiries vs. technical inquiries).
 - If the caller does not have the requisite authority, please inform the caller that you cannot assist him during the call. You may contact the authorized representative directly, or you may request that the caller ask the authorized representative contact you. Please do not release any information (including the name of the authorized representative) to the caller.

- If at any time you have reason to believe that the person you are speaking with either does not have the requisite authority or is not who he or she purports to be, please do not release any information to the caller. Instead, you may call the authorized representative on file at the **telephone number of record**.

*For purposes of the FCC's CPNI rules, the term **telephone number of record** is defined as the telephone number associated with the underlying service, not the telephone number supplied as a customer's "contact information."*

- **Inquiries Via Email:** A customer's email address must be verified on all incoming email inquiries.
 - Upon receipt of an email inquiry, please confirm that the writer's name and email address correspond with the designated authorized account representative and **email address of record** for that customer.

*For purposes of the FCC's CPNI rules, the term **address of record** means an address, whether postal or electronic, that the carrier has associated with the customer's account for at least 30 days.*

- Please confirm that the writer is authorized to act on behalf of the company for the requested information.
- If the writer is not authorized to act on behalf of the company or if the email address does not match the address of record listed in the company's contact information, please notify the writer that you may not assist him with the requested information. Please contact the authorized representative listed on the account or ask the writer to have the authorized representative contact you. Please do not release any information (including the name of the authorized representative) to the writer.

Verification Procedures for Professional Fault Management/Network Operating Center (Technical Support)

The verification procedures in this section apply to all personnel in Professional Fault Management/Network Operating Center ("NOC") and are intended to be read in conjunction with the established NOC procedures. If you receive a request from a customer to open a trouble ticket and you are not a member of the NOC, please transfer the call to the NOC for assistance. The verification procedures in this section apply to all requests to open trouble tickets, whether received through an incoming call or email.

- **Verification Procedures for Voice Customers:** DTNA only provides voice services to carrier customers. Upon commencement of service, DTNA provides a unique code to each carrier customer and a designated signaling point code. Upon receipt of a request to initiate a trouble ticket, the NOC representative must obtain the following information from the customer: (1) name, (2) company name, (3) unique code, and (4) signaling point code. If the requestor is unable to provide each of the items listed above, then the DTNA representative may not—and, as a technical matter, cannot—proceed with the call.

- Verification Procedures for Transport Customers: Upon receipt of a request to initiate a trouble ticket for a transport service, the NOC representative must obtain the following information from the customer: (1) name, (2) company name, (3) the circuit ID (e.g., 08x/4711); (4) the destination (A and B site); and (5) the class of service (e.g., Frame Relay). If the requestor is unable to provide each of the items listed above or the NOC representative has any concerns regarding the requestor's identity, the NOC representative may call the customer at the telephone number of record to proceed with providing technical support.

Verification Procedures for All Other Employees

If you receive a call from a customer and you are neither an employee in Sales and Customer Support or in Professional Fault Management, please refer the caller to either of those departments (as applicable) for assistance.

III. DISCLOSING CALL DETAIL INFORMATION UPON CUSTOMER REQUEST

Once DTNA has verified a customer's identity using the procedures discussed above, the DTNA representative may discuss certain information about the account with the caller. The DTNA representative also may make certain changes to the account as outlined in Part IV of this document.

All DTNA personnel are prohibited from releasing **Call Detail Information** (defined below) to any customer during an in-bound call. If a DTNA representative receives a request for **Call Detail Information**, he/she may provide that information to the caller by sending the information to the **address of record** or by calling the customer at the **telephone number of record**.

An address of record is not valid until it has been associated with the account for at least 30 days. Therefore, if you receive a request for call detail information within 30 days of the customer becoming a DTNA customer or within 30 days of a change of address request, you must send the information to the address of record.

*For purposes of the FCC's rules, the term **call detail information** is any information that pertains to the transmission of specific telephone calls, including, for outbound calls, the number called, and the time, location, or duration of any call and, for inbound calls, the number from which the call was placed, and the time, location, or duration of any call.*

The prohibition on the release of Call Detail Information during an in-bound call does not prevent a DTNA representative from addressing routine service and billing disputes during an in-bound call. As long as the caller provides the DTNA representative with the call detail information necessary to address the service issue, the DTNA representative may assist the customer with the inquiry. The DTNA representative simply cannot disclose any call detail information to the customer other than the call detail information that the customer already has disclosed.

If a customer has not received its bill and requests a duplicate copy of the bill, then you may send a copy of the bill via regular mail or email to the **address of record**.

If the customer claims to have moved to a new location, please inform the caller that he must submit a change of address request (see Part IV for the procedures to submit such a request) and that you cannot provide the requested billing information until you have received the change of address form and waited the requisite thirty-day period.

IV. ACCOUNT MODIFICATIONS

Once a DTNA representative has verified a customer's identity using the procedures outlined above, he/she may make certain changes to the account. If you receive a request to make an account modification discussed herein or to add/delete services to an account and you are not Sales and Support Personnel, please transfer the caller to Sales Support for assistance.

Under federal law, DTNA is required to notify its customers *immediately* of any creation or change of any address of record (whether electronic or postal). DTNA representatives must confirm all to a customer's address of record in writing immediately following the change by sending a letter to the customer at the *previous* address of record. It is DTNA's policy to notify customers of other changes to their accounts as set forth in this section.

Change of Postal Address of Record

- Step 1: Verify the customer's identity in accordance with the procedures outlined in Part II.
- Step 2: Verify the address of record.
- Step 3: Inform the customer that a change of billing address of record only can be made in writing. Please inform the customer that if he/she would like to continue to change the address, then he/she should send a written request *on company letterhead* to Sales and Support Personnel. The letter must be signed by an authorized point of contact and must include the following information:
 - Customer name;
 - Account number;
 - Address of record; and
 - New billing address.
- Step 4: The DTNA representative should change the address upon receipt of the appropriate documentation. Please ensure that the change of address is communicated to the billing department.

- Step 5: Once DTNA has processed the change of address, we will send a confirmation letter to the **old** billing addresses of record notifying the customer that it has changed its address of record.
- NOTE: Under federal law, an address of record must be associated with an account for thirty days before it is valid. Therefore, you must wait thirty days before sending any CPNI (such as call detail records or invoices) to the new address of record.

Addition of Authorized Representative

- Step 1: Verify the customer's identity in accordance with the procedures outlined in Part II.
- Step 2: Only the authorized point of contact may add an account representative.
- Step 3: Inform the caller that the addition of an authorized point of contact only can be made in writing. Please inform the customer that if he/she would like to continue with the addition of an authorized account representative, then he/she should mail a written request ***on company letterhead*** to Sales and Support Personnel.
- Step 4: The designated Sales Trader or Voice Trader (as applicable) should add the authorized point of contact upon receipt of the appropriate documentation from the customer. After updating the account information, please send a letter to the designated point of contact confirming the additional point of contact. ***It is imperative that you not release any information to the new point of contact until after DTNA has received the request in writing from the customer.***

Change of Authorized Representative

- Step 1: Verify the customer's identity in accordance with the procedures outlined in Part II.
- Step 2: Verify the name of the previous authorized account representative.
- Step 3: Inform the caller that a change of the account point of contact only can be made in writing. Please inform the customer that if he/she would like to continue to change the name of the account representative, then he/she should mail or fax a written request ***on company letterhead*** to the designated Sales Trader or Voice Trader. The letter must be signed and must include the following information:
 - Customer name;
 - Account number;
 - Current billing address;
 - Name of current account point of contact; and
 - Name of new account point of contact.

- Step 4: Send a letter to the current authorized contact(s) at the company's address of record. It is imperative that you not release any information to the new representative until after DTNA has received the request in writing from the customer.

Change of Services/Pricing on the Account or Requests for Disconnection

Any request for change of services (including additional or reduced routes on the account) or pricing must be addressed by the assigned Sales Trader or Voice Trader in conjunction with the legal department and must be made in writing. Any request for disconnection also must be addressed by the assigned Sales Trader or Voice Trader and must be made in writing.

If the Sales Trader or Voice Trader is unavailable, please request information from the caller regarding the inquiry, and send an email to the assigned Sales Trader or Voice Trader requesting that he/she contact the customer.

V. USE OF CPNI FOR MARKETING PURPOSES

All marketing campaigns must receive prior approval from the Head of Marketing. The Head of Marketing will maintain a record of all marketing campaigns that use CPNI in accordance with the FCC's specifications. If you seek approval to use CPNI for marketing purposes, please provide Jason Bennett with a proposed description of the campaign, the CPNI that you intend to use in the campaign, and what products and services you intend to offer in the campaign.

In accordance with the CPNI Protection Policy, currently all employees are prohibited from using CPNI to market services to customers outside of the category of service to which the customer already subscribes. If DTNA later decides to use CPNI to market products and services to customers outside of the category of service to which the customer subscribes, then we will provide notice to our customers advising them of their right to approve or disapprove of the use of their CPNI for certain marketing purposes. The Head of Marketing will maintain and manage a list of all customers who wish to and do not wish to be contacted. The legal department will assist the Head of Marketing in this capacity.

VI. PERMITTING ACCESS TO OR DISCLOSING CPNI TO THIRD PARTIES OR AFFILIATES

All employees also are prohibited from permitting access to or disclosing any CPNI to any third party for any purpose except as permitted under this manual. All employees also are prohibited from permitted access to or disclosing any CPNI to any affiliate, including T-Systems North America, Inc., unless explicitly authorized under this manual or by the legal department.

VII. REQUESTS FOR CPNI FROM LAW ENFORCEMENT PERSONNEL AND PERSONS OTHER THAN THE CUSTOMER

All requests for CPNI from any person other than the customer or the customer's authorized representative, including from law enforcement personnel, will be handled by David Friedman,

General Counsel. If you receive a written request for CPNI from any person other than the customer or the customer's authorized representative, please forward the request to David Friedman. If you receive an oral request from any person other than the customer or the customer's authorized representative, please ask that person to call David Friedman at (212) 301-6014.

A request for CPNI includes, but is not limited to, a request for a particular customer or customers' call records. A request for CPNI would include, for example, a request from an attorney claiming to have a valid subpoena for the information. A request from law enforcement personnel may come from a federal or state law enforcement agency, including, but not limited to, the United States Department of Justice, the Federal Bureau of Investigation, the Federal Communications Commission, and the police department. For purposes of this category, law enforcement personnel also include local state agencies, such as the school board. David Friedman will review all requests for CPNI from persons other than the customer or the customer's authorized representative.

It is DTNA's policy not to release any CPNI to any law enforcement personnel or to any person (other than the customer) claiming a right to the information absent a validly issued written subpoena. Any person or entity requesting CPNI orally will be asked to put the request in writing and to direct that request to David Friedman.

VIII. SECURITY BREACHES

DTNA will maintain a record of all security breaches discovered. DTBA will notify the United States Secret Service and the Federal Bureau of Investigation as well as its affected customers of any breaches in accordance with the FCC's rules. For purposes of this manual, a breach has occurred "when a person, without authorization or exceeding authorization, has intentionally gained access to, used, or disclosed CPNI." 47 C.F.R. § 64.2011(e). If you believe or suspect that a breach has occurred that has resulted in the unauthorized disclosure of CPNI, please contact David Friedman immediately. All notifications will be handled through Mr. Friedman; if you are aware of a security breach or if you suspect a security breach, please do not contact the customer directly. If the customer suspects that there has been a breach, please refer the call to Mr. Friedman. The legal department will maintain a record of all security breaches and customer notifications as required by the FCC's rules.

IX. ADDITIONAL SAFEGUARDS

As part of DTNA's obligations under U.S. law, DTNA tracks all customer complaints that it receives alleging the improper use, disclosure, or access to CPNI. If you receive a complaint from a customer (whether oral or written) regarding the alleged improper use, disclosure, or access to CPNI, please refer that complaint to the legal department.

DTNA also has an obligation to discover attempts that pretexters may take to gain unauthorized access to CPNI. If you become aware of any pretexting attempts or of any means that pretexters

may be using to attempt to gain access to a customer's CPNI, please immediately notify the legal department.

DTNA has implemented network security measures to secure its networks. If you become aware of any attempts to breach the network security, even if such attempt does not rise to the level of a security breach that results in the unauthorized release of CPNI (see section VIII), please immediately notify the legal department.

Appendix

Account information: information that is specifically connected to the customer's service relationship with the carrier, including such things as an account number or any component thereof, the telephone number associated with the account, or the bill's amount.

Address of record: whether postal or electronic, is an address that the carrier has associated with the customer's account for at least 30 days.

Call Detail Information: any information that pertains to the transmission of specific telephone calls, including, for outbound calls, the number called, and the time, location, or duration of any call and, for inbound calls, the number from which the call was placed, and the time, location, or duration of any call.

Communications-related services: telecommunications services, information services typically provided by telecommunications carriers, and services related to the provision or maintenance of customer premises equipment.

Opt-in approval: a method for obtaining customer consent to use, disclose, or permit access to the customer's CPNI. This approval method requires that the carrier obtain from the customer affirmative, express consent allowing the requested CPNI usage, disclosure, or access after the customer is provided appropriate notification of the carrier's request for consent consistent with the rules in this subpart.

Opt-out approval: a method for obtaining customer consent to use, disclose, or permit access to the customer's CPNI. Under this approval method, a customer is deemed to have consented to the use, disclosure, or access to the customer's CPNI if the customer has failed to object thereto within the thirty (30) day waiting period after the customer is provided appropriate notification of the carrier's request for consent.

Telephone number of record: the telephone number associated with the underlying service, not the telephone number supplied as a customer's "contact information."