Red Flag Rules Compliance Policy

This Red Flag Rules Compliance Policy for TelServ Communication Services LLC D/B/A HugeUC (“COMPANY”) contains guidelines for compliance with the Federal Trade Commission’s ("FTC") "Red Flag Rules," and establishes an Identity Theft Detection, Prevention, and Mitigation Program ("Program") [Part I, below] and a policy for addressing discrepancies in consumer reports [Part II, below] for COMPANY. COMPANY is a telecommunications service provider regulated by various state public utility commissions ("PUCs") and the Federal Communications Commission ("FCC").

The FTC’s Red Flag Rules were published in the Federal Register on November 9, 2007, and some of the rules became effective on November 1, 2008. Other aspects of the rules are effective November 1, 2009. The Red Flag Rules applicable to telecommunications carriers are summarized in 16 C.F.R. Section 681, and Appendix A to Section 681. COMPANY has reviewed these authorities and has fashioned a Program that complies with the Red Flag Rules’ requirements. The Program described in this Policy is designed to work in concert with COMPANY’s policy regarding the protection of Customer Proprietary Network Information ("CPNI"). COMPANY’s CPNI policy is embodied in a separate, written policy designed to protect and regulate the use of CPNI and other confidential subscriber information. This policy is contained in COMPANY’s Customer Proprietary Network Information Policy ("CPNI Policies").

Part I

Identity Theft Mitigation Policy

I. Purpose and Effective Date of the Program.

As an entity that collects, stores, and grants access to certain confidential subscriber information, COMPANY has taken steps to identify "red flags" that may be indicators of possible efforts by third parties to obtain unauthorized access to that information. COMPANY is committed to protecting their customers' privacy, and, as such, COMPANY has implemented procedures to detect possible efforts to engage in identity theft. COMPANY has designed their procedures to help prevent identity theft, and to help mitigate the effects of identity theft when it does occur. COMPANY's Red Flag Rules Program is effective April 1, 2021. Further details about the Program are set forth below.

II. Identifying Possible Identity Theft.

COMPANY is vigilant in identifying possible attempts at identity theft and other scams through which individuals might attempt to obtain unauthorized access to confidential information about COMPANY's customers. COMPANY's identification of possible "red flags" associated with identity theft includes consideration of the following indicators:

- News stories, alerts, notifications, warnings and other public information about identity theft scams, including any notifications from the FCC, the FTC, or the PUCs.

- The presentation of suspicious documents by customers in connection with service initiation, requests for account changes, or requests for access to account information, including the presentation of photo identification that does not match a customer's physical appearance, the presentation of documents that appear to be forged or altered, and/or the presentation of documents that appear to contain information that is inconsistent with other information that COMPANY has in its records regarding a customer.

- The presentation of suspicious personal identifying information in connection with service initiation, requests for account changes, or requests for access to account information. Multiple failed attempts to access COMPANY's online account system and multiple failed attempts to complete the authentication process for receiving access to account information will be considered "red flags" for the purpose of identifying possible identity theft.

- Unusual account activity, including material changes in payment patterns, calling patterns, and unusual modifications to account information.

- Multiple instances where a customer's mail is returned as undeliverable.

- Unusual activity in connection with adding or removing authorized individuals from an account.

- Account activity that is inconsistent with a customer's election not to permit publication of his or her telephone number and address.

- Where COMPANY has been notified by a customer, a regulatory agency, a credit reporting agency, or a law enforcement entity that a particular individual or account is at risk for identity theft.

None of these factors in isolation will be considered conclusive evidence that identity theft has occurred or will occur in the future, nor is this an exclusive list of the possible indicators of identity theft. However, the list of possible "red flags" above, considered together, reflects the most common set of indicators of possible identity theft that are relevant to COMPANY's circumstances and business models.

III. Detecting Possible Identity Theft.

In compliance with the FCC's rules governing CPNI, COMPANY has adopted written CPNI Policies, as described above. The customer authentication and authorization procedures described in the CPNI Policies are designed to protect against identity theft by controlling access to customers' account information, and by requiring

that customers be sufficiently authenticated prior to being given access to such information. Multiple failed authentications in connection with a single account may raise a "red flag" for identity theft. COMPANY's customer service representatives and employees in the business office who come into contact with customers are trained to report suspicious activity to their supervisors for further consideration. Supervisors have been instructed to report such suspicious activity to COMPANY's CPNI Compliance Officer as appropriate. The CPNI Compliance Officer will also be the primary point of contact for identify any "red flags" indicating possible identity theft in connection with this Red Flag Rules Program.

IV. Preventing and Mitigating Identity Theft.

COMPANY will evaluate each possible indicator of identity theft on a case-by-case basis as appropriate to protect COMPANY's customers and preserve the confidentiality of customers' account information. Although different responses will be appropriate in different cases, COMPANY will consider each of the following alternatives for addressing possible identity theft:

- Monitoring an account more closely to detect further evidence of identity theft.
- Contacting the affected customer to provide notice of the possible identity theft.
- Offering the affected customer the alternative to change his or her account password.
- Offering the affected customer the alternative to reopen an account under a new account number.
- Notifying law enforcement and/or relevant regulatory agencies of the possible identity theft.

COMPANY's CPNI Compliance Officer will determine whether one or more of the above responses, if any, is appropriate in a particular case.

COMPANY's procedures for notifying customers of account changes, and for notifying law enforcement and customers about CPNI breaches also help to prevent and mitigate possible identity theft. Further details about those procedures are provided in COMPANY's CPNI Policies.

V. Updates to the Identity Theft Detection, Prevention, and Mitigation Program.

COMPANY will evaluate its procedures for identifying possible identity theft on an annual basis. The review will be led by COMPANY's CPNI Compliance Officer in coordination with COMPANY's management and the supervisors of COMPANY's various business units. COMPANY will update this Policy as necessary to account for new identity theft scams and COMPANY's experiences in operating under this Policy.

VI. Administration of the Identity Theft Detection, Prevention, and Mitigation Program.

COMPANY's CPNI Compliance Officer will have primary responsibility for implementing and ensuring compliance with the Program. Each year, the CPNI Compliance Officer will prepare a report for review by COMPANY's management regarding material matters related to the program. The report will evaluate the effectiveness of the policies in the Program, identify any significant incidents involving identity theft and COMPANY's responses to such incidents. The report will also present any necessary recommendations regarding material changes to the program, including any recommendations regarding modifications to COMPANY's relationships with other service providers and outside vendors that may be appropriate to help protect against identity theft.

VII. Oversight of Relationships With Outside Vendors As Necessary to Protect Against Identity Theft.

As set forth in COMPANY's CPNI Policies, COMPANY will execute Non-Disclosure Agreements with outside vendors as necessary and applicable to protect CPNI and other confidential subscriber information. In addition to pursuing such agreements, COMPANY will evaluate its relationships and agreements with vendors to ensure that those relationships are structured to mitigate or reduce incidences of identity theft.

Part II

Consumer Report Discrepancy Policy:
Procedure for Responding to Address Discrepancy Notices Issued by Consumer Reporting Agencies

To the extent that COMPANY qualifies as "users of consumer reports" under the Fair Credit and Reporting Act, COMPANY will observe the following procedures in response to "notices of address discrepancy" from consumer reporting agencies. These procedures are effective April 1, 2021.

A. Definitions.

The definitions of terms used in this Policy will be the same as the definitions of terms in the Fair Credit Reporting Act, as codified in 15 U.S.C., Section 1681, et seq. The following specific definitions apply:

"Consumer report" is defined as "any written, oral, or other communication of any information by a consumer reporting agency bearing on a consumer's credit worthiness, credit standing, credit capacity, character, general reputation, personal characteristics, or mode of living which is used or expected to be used or collected in whole or in part for the purpose of serving as a factor in establishing the consumer's eligibility for credit or insurance to be used primarily for personal, family, or household purposes; employment purposes; or any other purpose authorized under 15 U.S.C., Section 1681b.

"Consumer reporting agency" is defined as "any person which, for monetary fees, dues, or on a cooperative nonprofit basis, regularly engages in whole or in part in the practice of assembling or evaluating consumer credit information or other information on consumers for the purpose of furnishing consumer reports to third parties, and which uses any means or facility of interstate commerce for the purpose of preparing or furnishing consumer reports."

A "notice of address discrepancy" includes any notice sent to COMPANY by a consumer reporting agency pursuant to 15 U.S.C. Section 1681c(h)(1) that informs COMPANY of a substantial difference between the address for the consumer that COMPANY provided to request a consumer report and the address or addresses in the agency's file for the consumer.

COMPANY will be considered a "user of consumer reports" if it relies on "consumer reports" issued by any "consumer reporting agencies" in making employment decisions, in assessing consumers' credit worthiness in connection with services purchased or requested from COMPANY, or for any other purpose authorized under the Fair Credit Reporting Act.

B. Investigation Upon Receipt of a Notice of Address Discrepancy.

Upon receipt of a notice of address discrepancy, COMPANY's CPNI Compliance Officer will conduct an investigation to determine the proper address of the consumer about whom COMPANY has sought a consumer report. The CPNI Compliance Officer will take all steps reasonably necessary to form a reasonable belief that the consumer report in question relates to the consumer about whom the consumer information was requested.

The CPNI Compliance Officer will use one or more of the following methods to resolve the address discrepancy, and form a reasonable belief that the consumer report is in fact related to the consumer for which it was sought:

1. Verifying the information in the consumer report provided by the consumer reporting agency with the consumer.

2. Comparing the information in the consumer report provided by the consumer reporting agency with information the user maintains in its own records, such as applications, change of address notifications, or other customer account records.

3. Comparing the information with information about the consumer from third-party sources that contain address information and other identifying information about the consumer.

C. Confirmation of Address With Consumer Reporting Agency.

Upon completion of the investigation described in Section B, above, the CPNI Compliance Officer will arrange for the correct address to be provided to the consumer reporting agency from whom the notice of address discrepancy was received. The CPNI Compliance Officer will furnish a consumer address to the consumer reporting agency only after COMPANY has reasonably confirmed that the address information is accurate through the methods described in Section B.

The address confirmation will be provided to the consumer reporting agency within a reasonable timeframe, in accordance with the reporting period in which it establishes a relationship with the consumer.