Analysis of Proposed Consent Order to Aid Public Comment *In the Matter of Global Tel*Link Corporation; Telmate, LLC; and TouchPay Holdings, LLC*, File No. 2123012

The Federal Trade Commission ("FTC" or "Commission") has accepted, subject to final approval, an agreement containing a consent order from Global Tel*Link Corporation, which also operates under the name Viapath ("Viapath"); Telmate, LLC ("Telmate"); and TouchPay Holdings, LLC ("TouchPay") (collectively, "Respondents").

The Proposed Order has been placed on the public record for thirty (30) days for receipt of comments by interested persons. Comments received during this period will become part of the public record. After thirty (30) days, the Commission will again review the agreement and the comments received, and it will decide whether it should withdraw from the agreement and take appropriate action or make final the agreement's Proposed Order.

Viapath is one of the largest providers of inmate telephone services in the United States. In combination with subsidiaries such as Telmate and TouchPay, Viapath also provides a host of additional communications, technology, and financial services to incarcerated consumers, their friends and family, and other outside contacts of incarcerated individuals, and to jails, prisons, and other carceral institutions ("Facility" or "Facilities").

In August 2020, a third-party contractor engaged by Telmate left a database containing consumers' personal information publicly exposed on the internet ("Incident"). The exposed database contained the personal information of thousands of people who used Respondents' products and services, including GettingOut, VisitNow (also known as VisitMe), Command, Telmate Inmate Telephone service, and Guardian.

The exposed personal information included the full text of messages exchanged using Respondents' services, grievance forms submitted by incarcerated people to jails and prisons, and information about incarcerated and non-incarcerated users such as names, dates of birth, phone numbers, usernames or email addresses in combination with passwords, home addresses, driver's license numbers, passport numbers, payment card numbers, financial account information, Social Security numbers, and data related to telephone services (like the dates and times of calls, called numbers, calling numbers, station used, and location information, like certain individuals' latitude and longitude at particular points in time). One or more unauthorized individuals accessed the exposed database and downloaded personal information from it. At least some of the exposed information was made available for sale on the dark web, where other people could also access or buy it.

The Commission's proposed six-count complaint alleges that Respondents violated Section 5(a) of the Federal Trade Commission Act by: (1) unfairly failing to employ reasonable data security measures (Count I); (2) unfairly failing to notify consumers affected by the Incident in a timely manner (Count II); (3) deceptively misrepresenting that Respondents implemented reasonable and appropriate measures to protect consumers' personal information against unauthorized access; (4) deceptively misrepresenting that Respondents had no reason to believe that consumers' sensitive personal information was affected by the Incident; (5) deceptively misrepresenting that Respondents would timely notify affected consumers; and (6) deceptively

misrepresenting that Respondents had never experienced a data security breach or that they had not experienced a data security breach within a particular timeframe that included the dates of the Incident.

Summary of Proposed Order with Respondents

The Proposed Order contains provisions designed to prevent Respondents from engaging in the same or similar acts or practices in the future. The Proposed Order also contains provisions designed to provide products to consumers affected by the Incident.

Provision I of the Proposed Order requires Respondents to establish and implement, and thereafter maintain, a comprehensive data security program that protects the security, confidentiality, and integrity of consumers' Personal Information, as that term is defined in the Proposed Order.

Provision II of the Proposed Order requires Respondents to obtain initial and biennial data security assessments by an independent third-party professional ("Assessor") for 20 years, and **Provision III** requires Respondents to cooperate with the Assessor in connection with the assessments required by Provision II.

Provision IV of the Proposed Order requires that a senior corporate manager or senior office of Respondents certify Respondents' compliance with the Proposed Order.

Provision V of the Proposed Order requires Respondents to provide consumers affected by the Incident with two years of enrollment in a credit monitoring and identity protection product. This provision includes requirements that are designed to help incarcerated consumers affected by the Incident access the product.

Provision VI of the Proposed Order requires Respondents to notify consumers and relevant Facilities of any future incident that results in Respondents notifying, pursuant to a statutory or regulatory requirement, any U.S. federal, state, or local government entity that Personal Information of or about an individual consumer was, or is reasonably believed to have been, accessed or acquired, or publicly exposed without authorization ("Covered Incident").

Provision VII of the Proposed Order requires Respondents to notify the Commission of any future Covered Incident.

Provision VIII of the Proposed Order prohibits Respondents from misrepresenting: (1) Respondents' privacy and security measures to prevent unauthorized access to Personal Information; (2) the occurrence, extent, nature, potential consequences, or any other fact relating to a Covered Incident actually or potentially involving or affecting Personal Information within the ownership, custody, or control of one or more Respondents; (3) the extent to which Respondents have notified or will notify affected parties in connection with a Covered Incident; (4) the extent to which Respondents meet or exceed industry-standard security or privacy practices; and (5) the extent to which Respondents otherwise protect the privacy, security, availability, confidentiality, or integrity of Personal Information.

Provision IX of the Proposed Order require Respondents to provide notice of the Incident by: (1) posting notice on each of Respondents' websites and the home screen of each of Respondents' mobile applications that has been used to provide Telmate products and services; and (2) sending notice to each consumer affected by the Incident that did not previously receive notification of the Incident. **Provision X** of the Proposed Order requires Respondents to provide relevant Facilities with notice of the Incident.

Provisions XI – XIV of the Proposed Order are reporting and compliance provisions, which include recordkeeping requirements and provisions requiring Respondents to provide information or documents necessary for the Commission to monitor compliance.

Provision XV states that the Proposed Order will remain in effect for twenty (20) years.