212-3012

UNITED STATES OF AMERICA
BEFORE THE FEDERAL TRADE COMMISSION

COMMISSIONERS: **Lina M. Khan, Chair**
Rebecca Kelly Slaughter
Alvaro M. Bedoya

In the Matter of **Global Tel*Link Corporation, a corporation, also d/b/a GTL, also d/b/a ViaPath Technologies;** **Telmate, LLC, a limited liability company, also d/b/a ViaPath Technologies; and** **TouchPay Holdings, LLC, a limited liability company, also d/b/a GTL Financial Services.**	**DECISION AND ORDER** **DOCKET NO. C-4801**

DECISION

The Federal Trade Commission ("Commission") initiated an investigation of certain acts and practices of the Respondents named in the caption. The Commission's Bureau of Consumer Protection ("BCP") prepared and furnished to Respondents a draft Complaint. BCP proposed to present the draft Complaint to the Commission for its consideration. If issued by the Commission, the draft Complaint would charge the Respondents with violations of the Federal Trade Commission Act.

Respondents and BCP thereafter executed an Agreement Containing Consent Order ("Consent Agreement"). The Consent Agreement includes: 1) statements by Respondents that they neither admit nor deny any of the allegations in the Complaint, except as specifically stated in this Decision and Order, and that only for purposes of this action, they admit the facts necessary to establish jurisdiction; and 2) waivers and other provisions as required by the Commission's Rules.

The Commission considered the matter and determined that it had reason to believe that Respondents have violated the Federal Trade Commission Act and that a Complaint should issue stating its charges in that respect. The Commission accepted the executed Consent Agreement and placed it on the public record for a period of 30 days for the receipt and consideration of public comments. The Commission duly considered any comments received from interested persons pursuant to Section 2.34 of its Rules, 16 C.F.R. § 2.34. Now, in further conformity with

the procedure prescribed in Rule 2.34, the Commission issues its Complaint, makes the following Findings, and issues the following Order:

Findings

1. The Respondents are:

    a. Respondent Global Tel*Link Corporation, a corporation, also doing business as GTL and as ViaPath Technologies ("GTL"), is an Idaho corporation with its principal office or place of business at 3120 Fairview Park Drive, Suite 300, Falls Church, Virginia, 22042.

    b. Respondent Telmate, LLC, also doing business as ViaPath Technologies, ("Telmate") is a Delaware limited liability company with its principal office or place of business at 3120 Fairview Park Drive, Suite 300, Falls Church, Virginia, 22042. Telmate is a wholly owned subsidiary of GTL.

    c. Respondent TouchPay Holdings, LLC, also doing business as GTL Financial Services, ("TouchPay") is a Texas limited liability company with its principal office or place of business at 10005 Technology Boulevard West, Suite 130, Dallas, Texas, 75220.

2. The Commission has jurisdiction over the subject matter of this proceeding and over the Respondents, and the proceeding is in the public interest.

ORDER

Definitions

For purposes of this Order, the following definitions apply:

A. "**Affected Consumer**" means any individual consumer whose Personal Information was exposed by the Identified Breach if:

    1. The exposed information includes any of the following with respect to the individual consumer (hereafter for purposes of this definition, "Identifying Elements"):

        a. An individual's first and last name, so long as it appears in conjunction with Personal Information other than a first and last name;

        b. A Social Security number (but not including only the last four digits of a Social Security number), driver's license number, passport number, alien registration number, or other government-issued unique identification number;

        c. A unique numeric identifier assigned to an individual by a Facility in connection with the individual's incarceration, such as a booking number;

d. A unique financial identifier, including a full financial account number, full credit or debit card number, or electronic identification number; or

e. An email address or other online contact information, such as a user identifier or a screen name;

2. Respondents have collected or maintained the exposed Identifying Elements in the ordinary course of business; and

3. Respondents have the technological capability to link the exposed Identifying Elements with the consumer's valid mail or email address or other means of communicating with the consumer in writing.

B. "**Authorized User**" means any employee, contractor, agent, customer, or other person that is authorized to access any of Respondents' information systems or data.

C. "**Change Management**" means a documented process for making changes that affect risk to the security of networks, systems, and assets that store, process, or connect to systems that store or process Personal Information, including the identification, impact analysis, approval or rejection, prioritization, implementation, testing, and post-implementation review of such changes.

D. "**Clear(ly) and conspicuous(ly)**" means that a required disclosure is difficult to miss (i.e., easily noticeable) and easily understandable by ordinary consumers, including in all of the following ways:

1. In any communication that is solely visual or solely audible, the disclosure must be made through the same means through which the communication is presented. In any communication made through both visual and audible means, such as a television advertisement, the disclosure must be presented simultaneously in both the visual and audible portions of the communication even if the representation requiring the disclosure ("triggering representation") is made through only one means.

2. A visual disclosure, by its size, contrast, location, the length of time it appears, and other characteristics, must stand out from any accompanying text or other visual elements so that it is easily noticed, read, and understood.

3. An audible disclosure, including by telephone or streaming video, must be delivered in a volume, speed, and cadence sufficient for ordinary consumers to easily hear and understand it.

4. In any communication using an interactive electronic medium, such as the Internet or software, the disclosure must be unavoidable.

6. The disclosure must use diction and syntax understandable to ordinary consumers and must appear in each language in which the triggering representation appears.

7. The disclosure must comply with these requirements in each medium through which it is received, including all electronic devices and face-to-face communications.

8. The disclosure must not be contradicted or mitigated by, or inconsistent with, anything else in the communication.

9. When the representation or sales practice targets a specific audience, such as children, the elderly, or the terminally ill, "ordinary consumers" includes reasonable members of that group.

E. "**Consumer Report**" has the meaning provided in the Fair Credit Reporting Act ("FCRA"), 15 U.S.C. § 1681 et seq., and any amendments thereto. As of the date of effective date of this Order, "Consumer Report" is defined under the FCRA 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: (1) credit or insurance to be used primarily for personal, family, or household purposes; (2) employment purposes; or (3) any other purpose authorized under FCRA Section 604, 15 U.S.C. § 1681b.

F. "**Consumer Reporting Agency**" has the meaning provided in the FCRA, 15 U.S.C. § 1681 et seq., and any amendments thereto. As of the date of effective date of this Order, "Consumer Reporting Agency" is defined under the FCRA 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.

G. "**Covered Incident**" means any 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.

H. "**Facility**" or "**Facilities**" means a Jail or Prison, and any entity with which Respondents contract to provide any product or service in connection with the operation of a Jail or Prison.

I. "**Future Affected Consumer**" means any individual consumer whose Personal Information Respondents have reason to believe has been accessed, acquired, or publicly exposed without authorization in connection with a Covered Incident if:

1. The accessed, acquired, or publicly exposed information includes any of the following (hereafter for purposes of this definition, "Identifying Elements"):

    a. An individual's first and last name, so long as it appears in conjunction with Personal Information other than a first and last name;

    b. A Social Security number (but not including only the last four digits of a Social Security number), driver's license number, passport number, alien registration number, or other government-issued unique identification number;

    c. A unique numeric identifier assigned to an individual by a Facility in connection with the individual's incarceration, such as a booking number;

    d. Unique biometric data such as a face embedding, fingerprint, voice print, a retina or iris image, or any other unique physical representation;

    e. A unique financial identifier, including a full financial account number, a full credit or debit card number, or electronic identification number; or

    f. An email address or other online contact information, such as a user identifier or a screen name;

2. Respondents have collected or maintained the accessed, acquired, or publicly exposed Identifying Elements in the ordinary course of business; and

3. Respondents have the technological capability to link the accessed, acquired, or publicly exposed Identifying Elements with the consumer's valid mail or email address or other means of communicating with the consumer in writing.

J. "**Identified Breach**" means the exposure of Personal Information from systems of or controlled by Respondents that was discovered on or about August 13, 2020.

K. "**Jail**" means a facility of a local, state, or federal law enforcement agency that is used primarily to hold individuals who are:

1. Awaiting adjudication of criminal charges;

2. Post-conviction and committed to confinement for sentences of one year or less; or

3. Post-conviction and awaiting transfer to another facility. The term also includes city, county, or regional facilities that have contracted with a private company to manage day-to-day operations; privately owned and operated facilities primarily engaged in housing city, county or regional inmates; facilities used to detain individuals, operated directly by the Federal Bureau of Prisons or U.S. Immigration and Customs Enforcement, or pursuant to a contract with those agencies; juvenile detention centers; and secure mental health facilities.

L. "**Multi-Factor Authentication**" means authentication through verification of at least two of the following types of authentication factors:

1. Knowledge factors, such as a password;

2. Possession factors, such as a token; or

3. Inherence factors, such as biometric characteristics.

M. "**Nationwide Consumer Reporting Agency**" means a Consumer Reporting Agency that regularly engages in the practice of assembling or evaluating, and maintaining, for the purpose of furnishing consumer reports to third parties bearing on a consumer's credit worthiness, credit standing, or credit capacity, each of the following regarding consumers residing nationwide:

1. Public record information; and

2. Credit account information from persons who furnish that information regularly and in the ordinary course of business.

N. "**Personal Information**" means information from or about an individual consumer, including (1) a first and last name; (2) a physical address; (3) an email address or other online contact information, such as a user identifier or a screen name; (4) a telephone number; (5) a financial account number in conjunction with information that can reasonably be used to identify the corresponding financial institution; (6) credit or debit card information (including a partial credit or debit card number consisting of more than 5 digits of the full credit or debit card number); (7) information about or derived from the individual's government-issued identification documents or credentials, such as an image of a driver's license, state identification card, or passport, or a driver's license number, military identification number, or Social Security number; (8) date of birth; (9) a persistent identifier, such as a customer number held in a "cookie," a static Internet Protocol ("IP") address, a mobile device ID, or device or component serial number; and (10) user account credentials, such as a login name and password (whether plain text, encrypted, hashed, and/or salted).

O. "**Prison**" means a facility operated by a territorial, state, or federal agency that is used primarily to confine individuals convicted of felonies and sentenced to terms in excess of one year. The term also includes public and private facilities that provide outsource housing to other agencies such as the State Departments of Correction and the Federal Bureau of Prisons; and facilities that would otherwise fall under the definition of a Jail but in which the majority of inmates are post-conviction and are committed to confinement for sentences of longer than one year.

P. "**Respondents**" means Respondents, individually, collectively, or in any combination.

Provisions

I. Mandated Information Security Program

IT IS FURTHER ORDERED that Respondents, and any business that Respondents control directly, or indirectly, in connection with the collection, maintenance, use, or disclosure of, or provision of access to, Personal Information, must, within sixty (60) days of the effective date of this Order, establish and implement, and thereafter maintain, a comprehensive information security program ("Information Security Program") that protects the security, confidentiality, and integrity of such Personal Information. To satisfy this requirement, Respondents must, at a minimum:

A. Document in writing the content, implementation, and maintenance of the Information Security Program;

B. Designate a qualified employee responsible for coordinating, overseeing, and implementing the Information Security Program and enforcing the Information Security Program ("Qualified Individual");

C. Require the Qualified Individual to report in writing to Respondents' board of directors or governing body or, if no such board or equivalent governing body exists, to a senior officer of Respondents responsible for Respondents' Information Security Program at least once every twelve (12) months and promptly (not to exceed thirty (30) days) after a Covered Incident, if any. The report must include the following information:

1. The overall status of the Information Security Program and Respondents' compliance with this Provision, including by providing the written program and any evaluations thereof or updates thereto; and

2. Material matters related to the Information Security Program, addressing issues such as risk assessment, risk management, and control decisions; service provider arrangements; results of testing, including any testing conducted pursuant to sub-Provision G of this Provision; Covered Incidents or violations of Respondents' information security policies or procedures and management's responses thereto; and recommendations for changes in the Information Security Program.

D. Assess and document, at least once every twelve (12) months and promptly (not to exceed thirty (30) days) following a Covered Incident, reasonably foreseeable internal and external risks to the security, confidentiality, or integrity of Personal Information within the possession, custody, or control of Respondents that could result in the (1) unauthorized collection, maintenance, use, or disclosure of, provision of access to, or destruction of, Personal Information; or (2) misuse, loss, theft, alteration, or other compromise of such information. The risk assessments must be written and must include:

1. Criteria for the evaluation and categorization of identified security risks or threats Respondents face;

2. Criteria for the assessment of the confidentiality, integrity, and availability of Respondents' networks, systems, and assets and Personal Information, including the adequacy of the existing controls in the context of the identified risks or threats Respondents face; and

3. Requirements describing how identified risks will be mitigated or accepted based on the risk assessment and how the Information Security Program will address the risks.

E. Design, implement, maintain, and document safeguards that control for the internal and external risks identified in response to sub-Provision I.D. Each safeguard must be based on the volume and sensitivity of the Personal Information that is at risk, and the likelihood that the risk could be realized and result in the (1) unauthorized collection, maintenance, use, or disclosure of, provision of access to, or destruction of, Personal Information; or (2) misuse, loss, theft, alteration, or other compromise of such information. Such safeguards must also include:

1. Policies, procedures, standards, and technical measures to systematically inventory Personal Information in Respondents' control, including policies, procedures, and technical measures to track and inventory the transfer and storage of Personal Information among and within Respondents' various networks, systems, and assets;

2. Policies, procedures, standards, and technical measures to log and monitor access to networks, systems, and assets in Respondents' control;

3. Policies, procedures, standards, and technical measures to monitor all of Respondents' networks, systems, and assets to identify and log anomalous activity and/or data security events, including unauthorized attempts to access or exfiltrate Personal Information from Respondents' networks, systems, and assets. Such measures must require Respondents to determine baseline system activity, identify and respond to anomalous events and unauthorized attempts to access or exfiltrate Personal Information, and verify the effectiveness of monitoring and logging;

4. Technical, organizational, and, as appropriate, physical controls to:

    a. Safeguard against unauthorized access to any network, system, or asset in Respondents' control that stores, collects, maintains, or processes Personal Information, including properly configured firewalls; intrusion detection and prevention systems configured to identify and prevent unauthorized access to networks, systems, or assets that store, process, or connect to networks, systems, or assets that store or process Personal Information; file integrity

monitoring tools; data loss prevention tools; properly configured physical or logical segmentation of networks, systems, and databases; restricting inbound connections to approved IP addresses; requiring that connections to the network, system, or asset are authenticated and encrypted; preventing the storage of unsecured access keys or other unsecured credentials on Respondents' networks, systems, or assets, or in any cloud-based services; requiring and enforcing strong passwords and other credentials; and

b. Limit Authorized Users' access only to Personal Information that they need to perform their duties and functions, or, in the case of consumers, to access their own information, periodically audit Authorized Users' levels of access based on their need to know, and terminate access within 30 days following a change in Authorized Users' need to know (including because of the termination of employment or contract) or if Authorized Users engage in inappropriate access or usage;

5. Policies and procedures to document in writing the content, implementation, and maintenance of an incident response plan designed to ensure the identification of, investigation of, and response to the unauthorized access to Personal Information. Such incident response plan must include policies and procedures to ensure the timely investigation of data security events and the timely remediation of critical and high-risk vulnerabilities. Respondents must revise and update this incident response plan to adapt to any changes to their networks, systems, and assets;

6. Regular security training programs, on at least an annual basis, that are updated, as applicable, to address internal or external risks identified by Respondents under sub-Provision I.D of this Order, and that include, at a minimum:

   a. Security awareness training for all employees and service providers who have access to networks, systems, or assets that contain Personal Information on Respondents' security policies and procedures, including the requirements of this Order, to be conducted when an employee begins employment or takes on a new role in which the employee has access to networks, systems, or assets that contain Personal Information, and on at least an annual basis thereafter;

   b. For information security personnel, security updates and training sufficient to address relevant security risks; and

   c. For developers, engineers, other employees, and service providers with job duties that relate to the development, design, implementation, updating, modification, or operation of systems or software that Respondents use to provide products or services, training in secure development principles, including secure engineering and defensive programming concepts;

7. Utilizing qualified information security personnel employed by Respondents or an

affiliate or service provider sufficient to manage Respondents' information security risks and to perform or oversee the Information Security Program, and verifying that key information security personnel take steps to maintain current knowledge of changing information security threats and countermeasures;

8. Protecting by encryption, at a minimum, all information about or derived from an individual's government-issued identification documents or credentials, such as an image of a driver's license, state identification card, or passport, or a driver's license number, military identification number, passport number, or Social Security number, dates of birth, messages exchanged by users, and user account credentials held or transmitted by Respondents both in transit over external networks and at rest, except that, to the extent Respondents determine that encryption of this information, either in transit over external networks or at rest, is infeasible or would increase the risk of unauthorized access to consumers' Personal Information, Respondents may instead secure such information using effective alternative compensating controls reviewed and approved by the Qualified Individual;

9. Adopting secure development practices and procedures for in-house developed applications utilized by Respondents for transmitting, accessing, or storing Personal Information and for evaluating, assessing, or testing the security of externally developed applications that Respondents utilize to transmit, access, or store Personal Information;

10. Adopting and implementing procedures for Change Management that apply to all networks, systems, and assets that contain Personal Information, which must include the following requirements as to each change subject to Change Management procedures:

    a. The change must be implemented by applying source code or configuration files to a network, system, or asset;

    b. The source code or configuration files required by sub-Provision I.E.10.a must be reviewed and approved, prior to their application, by a person with appropriate training or expertise other than the person proposing, planning, or implementing the change; and

    c. The means by which the reviewed code or configuration files are applied must be programmatic or automated, rather than manual, unless:

        i. The Qualified Individual makes a written determination that programmatic or automated application is impossible, and that such impossibility cannot be remedied without increased risk of unauthorized access to consumers' Personal Information; and

        ii. Respondents develop and implement alternative procedures, specifically approved and documented by the Qualified Individual, to ensure that the

manual application of reviewed code or configuration files does not result in the introduction of error.

11. Requiring Multi-Factor Authentication for any of Respondents' employees or contractors to access any information system in Respondents' control that is used, in whole or in part, to store, collect, or transmit Personal Information, unless the Qualified Individual has approved in writing the use of reasonably equivalent or more secure access controls; and

12. Developing, implementing, and maintaining policies and procedures to minimize data collection, storage, and retention, including data deletion or retention policies and procedures. Such policies and procedures must include the secure disposal of Personal Information in any format no later than two years after the last date the information is used in connection with the provision of a product or service to the consumer to which it relates, unless such information is necessary for business operations or for other legitimate business purposes, including to comply with a properly authorized civil, criminal, or regulatory investigation, or subpoena or summons by Federal, state, or local authorities; to comply with the consumer's request; where the information is otherwise required to be retained by law or regulation; or where targeted disposal is not reasonably feasible due to the manner in which the information is maintained. To the extent Respondents retain information for longer than two years after the last date the information is used in connection with the provision of a product or service to the consumer to which it relates, Respondents must document in writing the legitimate business purpose for which Respondents retain such information and must delete such information upon the conclusion of the stated business purpose. Respondents must periodically review Respondents' data retention policy to minimize the unnecessary retention of data;

F. Assess, at least once every twelve (12) months and promptly (not to exceed thirty (30) days) following a Covered Incident, the sufficiency of any safeguards in place to address the internal and external risks to the security, confidentiality, or integrity of Personal Information, and modify the Information Security Program based on the results;

G. Test and monitor the effectiveness of the safeguards at least once every twelve (12) months and promptly (not to exceed thirty (30) days) following a Covered Incident, and modify the Information Security Program based on the results. Such testing and monitoring must include vulnerability testing of Respondents' networks, systems, and assets once every four (4) months and promptly (not to exceed thirty (30) days) after a Covered Incident, and penetration testing of Respondents' networks, systems, and assets at least once every twelve (12) months and promptly (not to exceed thirty (30) days) after a Covered Incident;

H. Select and retain service providers capable of safeguarding Personal Information they access through or receive from Respondents, including by implementing policies and procedures to adequately vet and assess the service providers' data security practices

prior to contracting with the service providers and periodically thereafter. Respondents must also contractually require service providers to (1) provide regular security training programs to their employees; and (2) implement and maintain safeguards sufficient to address the internal and external risks to the security, confidentiality, or integrity of Personal Information; and

I. Evaluate and adjust the Information Security Program in light of any material changes to Respondents' operations or business arrangements, a Covered Incident, new or more efficient technological or operational methods to control for the risks identified in Provision I.D of this Order, or any other circumstances that Respondents know or have reason to know may have an impact on the effectiveness of the Information Security Program or any of its individual safeguards. At a minimum, Respondents must evaluate the Information Security Program at least once every twelve (12) months and modify the Information Security Program based on the results.

Provided, however, that nothing in this Order shall prohibit Respondents' authorized publication or disclosure, including in plain text, of an incarcerated person's Personal Information to the extent that a Facility requires such disclosure by contract or for the purpose of locating, identifying, communicating with, or depositing funds for the use of such incarcerated person.

II. Information Security Assessments by a Third Party

IT IS FURTHER ORDERED that, in connection with compliance with Provision I of this Order, titled Mandated Information Security Program, Respondents must obtain initial and biennial assessments ("Assessments"):

A. The Assessments must be obtained from a qualified, objective, independent third-party professional ("Assessor"), who (1) uses procedures and standards generally accepted in the profession; (2) conducts an independent review of the Information Security Program; and (3) retains all documents relevant to each Assessment for five (5) years after completion of such Assessment and will provide such documents to the Commission within ten (10) days of receipt of a written request from a representative of the Commission. The Assessor may not withhold any documents relating to Assessments of Respondents from the Commission on the basis of a claim of confidentiality, proprietary or trade secrets, work product protection, attorney-client privilege, statutory protection, or any similar claim.

B. For each Assessment, Respondents must provide the Associate Director for Enforcement for the Bureau of Consumer Protection at the Federal Trade Commission with the name, affiliation, and qualifications of the proposed Assessor, whom the Associate Director will have the authority to approve in her or his sole discretion.

C. The reporting period for the Assessments must cover (1) the first 180 days after the issuance date of the Order for the initial Assessment; and (2) each two-year period thereafter for twenty (20) years after issuance of the Order for the biennial

Assessments.

D. Each Assessment must, for the entire assessment period:

1. Determine whether Respondents have implemented and maintained the Information Security Program required by Provision I of this Order, titled Mandated Information Security Program;

2. Assess the effectiveness of Respondents' implementation and maintenance of sub-Provisions I.A-I;

3. Identify any gaps or weaknesses in, or instances of material noncompliance with, the Information Security Program;

4. Address the status of gaps or weaknesses in, or instances of material non-compliance with, the Information Security Program that were identified in any prior Assessment required by this Order; and

5. Identify specific evidence (including documents reviewed, sampling and testing performed, and interviews conducted) examined to make such determinations, assessments, and identifications, and explain why the evidence that the Assessor examined is (a) appropriate for assessing an enterprise of Respondents' size, complexity, and risk profile; and (b) sufficient to justify the Assessor's findings. No finding of any Assessment shall rely primarily on assertions or attestations by Respondents' management. The Assessment must be signed by the Assessor, state that the Assessor conducted an independent review of the Information Security Program and did not rely primarily on assertions or attestations by Respondents' management, and state the number of hours that each member of the assessment team worked on the Assessment. To the extent that Respondents revise, update, or add one or more safeguards required under Provision I of this Order during an Assessment period, the Assessment must assess the effectiveness of the revised, updated, or added safeguard(s) for the time period in which it was in effect, and provide a separate statement detailing the basis for each revised, updated, or additional safeguard.

E. Each Assessment must be completed within sixty (60) days after the end of the reporting period to which the Assessment applies. Unless otherwise directed by a Commission representative in writing, Respondents must submit an unredacted copy of the initial Assessment and a proposed redacted copy suitable for public disclosure to the Commission within ten (10) days after the Assessment has been completed via email to DEbrief@ftc.gov or by overnight courier (not the U.S. Postal Service) to Associate Director for Enforcement, Bureau of Consumer Protection, Federal Trade Commission, 600 Pennsylvania Avenue NW, Washington, DC 20580. The subject line must begin, "In re Global Tel*Link Corporation, FTC File No. 2123012." Respondents must retain an unredacted copy of each subsequent biennial Assessment as well as a proposed redacted copy of each subsequent biennial Assessment suitable

for public disclosure until the order is terminated and must provide each such Assessment to the Associate Director for Enforcement within ten (10) days of request. The initial Assessment and any subsequent biennial Assessment provided to the Commission must be marked, in the upper right-hand corner of each page, with the words "DPIP Assessment" in red lettering.

III. Cooperation with Third-Party Information Security Assessor

IT IS FURTHER ORDERED that Respondents, whether acting directly or indirectly, in connection with any Assessment required by Provision II of this Order, titled Information Security Assessments by a Third Party, must:

A. Provide or otherwise make available to the Assessor all information and material in their possession, custody, or control that is relevant to the Assessment for which there is no reasonable claim of privilege;

B. Provide or otherwise make available to the Assessor information about Respondents' network(s), systems, and assets so that the Assessor can determine the scope of the Assessment, and visibility to those portions of the network(s), systems, and assets deemed in scope; and

C. Disclose all material facts to the Assessor, and not misrepresent in any manner, expressly or by implication, any fact material to the Assessor's (1) determination of whether Respondents have implemented and maintained the Information Security Program required by Provision I of this Order, titled Mandated Information Security Program; (2) assessment of the effectiveness of the implementation and maintenance of sub-Provisions I.A-I; or (3) identification of any gaps or weaknesses in, or instances of material noncompliance with, the Information Security Program.

IV. Annual Certification

IT IS FURTHER ORDERED that, Respondents must:

A. One year after the issuance date of this Order, and each year thereafter, provide the Commission with a certification from a senior corporate manager, or, if no such senior corporate manager exists, a senior officer of Respondents responsible for Respondents' Information Security Program that (1) Respondents have established, implemented, and maintained the requirements of this Order; (2) Respondents are not aware of any material noncompliance that has not been (a) corrected or (b) disclosed to the Commission; and (3) includes a brief description of all Covered Incidents during the certified period. The certification must be based on the personal knowledge of the senior corporate manager, senior officer, or subject matter experts upon whom the senior corporate manager or senior officer reasonably relies in making the certification.

B. Unless otherwise directed by a Commission representative in writing, submit all

annual certifications to the Commission pursuant to this Order via email to DEbrief@ftc.gov or by overnight courier (not the U.S. Postal Service) to Associate Director for Enforcement, Bureau of Consumer Protection, Federal Trade Commission, 600 Pennsylvania Avenue NW, Washington, DC 20580. The subject line must begin: "In re Global Tel*Link Corporation, FTC File No. 2123012."

V. Credit Monitoring and Identity Protection Product

IT IS FURTHER ORDERED that Respondents must provide Affected Consumers enrollment in a credit monitoring and identity protection product (the "Product") as set forth below:

A. The Product must be offered, provided, and maintained by an independent third party (the "Third Party") that has been approved by the Associate Director for Enforcement for the Bureau of Consumer Protection at the Federal Trade Commission. Within 14 days of the effective date of this Order, Telmate and its successors and assigns must provide the name and qualifications of the Third Party to: DEbrief@ftc.gov or sent by overnight courier (not the U.S. Postal Service) to: Associate Director for Enforcement, Bureau of Consumer Protection, Federal Trade Commission, 600 Pennsylvania Avenue NW, Washington, DC 20580. The subject line must begin: "In re Global Tel*Link Corporation, FTC File No. 2123012."

B. Within one hundred and twenty (120) days of receiving approval of the Third Party from the Associate Director for Enforcement for the Bureau of Consumer Protection, Telmate and its successors and assigns must:

    1. Instruct or otherwise cause the Third Party to provide to each Affected Consumer receiving a notice pursuant to Section IX.B the means to register for or access the Product, such as an activation code; and

    2. Provide the Third Party with sufficient information regarding Affected Consumers to enable the Third Party to efficiently identify and communicate with each Affected Consumer, including, to the extent known, information regarding whether any Affected Consumer is currently incarcerated; if so, in what Facility.

C. After complying with sub-Provision B of this Provision, Telmate and its successors and assigns must, within thirty (30) days of learning the identity of an additional Affected Consumer, learning of any reason to believe that an Affected Consumer has not received the means to register for or access the Product, instruct or otherwise cause the Third Party to provide each such Affected Consumer with the means to register for or access the Product.

D. Telmate and its successors and assigns must require the Third Party to communicate with each Affected Consumer using methods of communication that are reasonably calculated to reach that consumer, including in light of the consumer's incarceration status. The

Third Party must be able to send and receive communications to and from consumers by mail.

E. To the extent that Respondents provide communications services, including voice or telephone services or services related to incarcerated consumers' ability to send and receive mail, in any Facility in which any Affected Consumer is incarcerated, Respondents will coordinate in good faith with Facilities to allow Affected Consumers who are incarcerated to enroll in the Product via those communication services, including by requesting that Facilities add a telephone number that can be used for enrollment in the Product to the approved call list. Respondents will make reasonable efforts to ensure that calls and mail between Third Party and Affected Consumers are free of charge.

F. Affected Consumers must be eligible to enroll in the Product for a period of at least ninety (90) days following receipt of information from the Third Party about how to register for or access the Product. Telmate and its successors and assigns must cause the Third Party to provide each such Affected Consumer with two (2) years of enrollment in the Product beginning on the date that the Affected Consumer registers for the Product.

G. The Product must include:

1. An option for Affected Consumers incarcerated in Facilities to receive automated credit monitoring alerts generated by the Product via a mechanism that is simple, accessible, secure, and free of charge to Affected Consumers and the Third Party, such as by providing a mechanism by which Affected Consumers can receive alerts by mail;

2. Daily Consumer Report monitoring from each of the three Nationwide Consumer Reporting Agencies showing key changes to one or more of an Affected Consumer's Consumer Reports, including automated alerts when the following occur: new accounts are opened; inquiries or requests for an Affected Consumer's Consumer Report for the purpose of obtaining credit, including for new credit card applications; changes to an Affected Consumer's address; and negative information, including delinquencies or bankruptcies;

3. Automated alerts, using public or proprietary data sources:

    a. When data elements submitted by an Affected Consumer for monitoring, such as Social Security numbers, email addresses, or credit card numbers, appear on suspicious websites, including websites on the "dark web;"

    b. When names, aliases, and addresses have been associated with the Affected Consumer's Social Security number in connection with information reported to the Consumer Reporting Agencies;

    c. When a payday loan or certain other unsecured credit has been taken or opened using the Affected Consumer's Social Security number;

d. When banking activity is detected related to new deposit account applications, opening of new deposit accounts, changes to an Affected Consumer's personal information on an account, and new signers being added to an Affected Consumer's account; and

e. When a balance is reported on an Affected Consumer's credit line that has been inactive for at least six months;

4. One Million Dollars ($1,000,000) in identity theft insurance to cover costs related to incidents of identity theft or identity fraud, with coverage prior to the Affected Consumer's enrollment in the Product, provided the costs result from a stolen identity event first discovered during the policy period and subject to the terms of the insurance policy;

5. A customer service center to provide assistance with enrollment, website navigation, monitoring alerts questions, dispute assistance, fraud resolution assistance, and other assistance related to the Product;

6. For Affected Consumers under the age of 18, the Product includes child monitoring services where the parent or guardian can enroll the Affected Consumer under the age of 18 to receive the following services: alerts when data elements submitted for monitoring appear on suspicious websites, such as websites on the "dark web;" and alerts when the Social Security number of an Affected Consumer under the age of 18 is associated with new names or addresses or the creation of a Consumer Report at one or more of the three Nationwide Consumer Reporting Agencies.

H. Respondents must not receive or retain any monetary benefit from the Product.

VI. Covered Incident Notification to Consumers and Facilities

IT IS FURTHER ORDERED that, following any future Covered Incident, Respondents must make reasonable efforts to identify each Future Affected Consumer and must provide notification to each identified Future Affected Consumer as follows:

A. Within thirty (30) days of any notification to a United States federal, state, or local entity of a Covered Incident, Respondents must provide, to each Future Affected Consumer, a notice including:

1. The date, estimated date, or estimated date range when the Covered Incident occurred;

2. A description of the facts relating to the Covered Incident, including the causes of the Covered Incident, if known (unless otherwise prohibited by law);

3. A description of each type of Personal Information that Respondents have reason to

believe was accessed, acquired, or publicly exposed without authorization in connection with the Covered Incident;

4. The acts that Respondents have taken to date to remediate the Covered Incident and protect Personal Information from further exposure, acquisition, or access;

5. Information that a consumer can use to contact Respondents to inquire about the Covered Incident;

6. A statement that the consumer can obtain information from the Federal Trade Commission ("FTC") and the Nationwide Consumer Reporting Agencies about fraud alerts and security freezes; and

7. The up-to-date toll-free numbers, addresses, and websites for the Nationwide Consumer Reporting Agencies and the FTC; and

B. Within thirty (30) days of any notification to a United States federal, state, or local entity of a Covered Incident, Respondents must provide to (1) each Facility that is associated with the Personal Information that is accessed, acquired, or publicly exposed without authorization and (2) each Facility in which Respondents know that one or more Future Affected Consumers is incarcerated at the time of the Covered Incident (each a "Future Affected Facility"):

1. The date, estimated date, or estimated date range when the Covered Incident occurred;

2. A description of the facts relating to the Covered Incident, including the causes of the Covered Incident, if known;

3. A description of each type of Personal Information that Respondents have reason to believe was accessed, acquired, or publicly exposed without authorization in connection with the Covered Incident;

4. The number of Future Affected Consumers and the number of Future Affected Consumers with a known relationship to the Facility;

5. An explanation of how the Facility can obtain more information about which consumers were affected by the Covered Incident and steps the Facility can take to assist Future Affected Consumers; and

6. The acts that Respondents have taken to date to remediate the Covered Incident and protect Personal Information from further exposure or access;

C. If Respondents identify an additional Future Affected Consumer more than thirty (30) days following the Covered Incident, Respondents must provide to the Future Affected

Consumer, within thirty (30) days of such identification, a notice including the elements listed at sub-Provision VI.A.1-7, and to each Future Affected Facility, if any, that has not previously been notified pursuant to sub-Provision VI.B., a notice including the elements listed at sub-Provision VI.B.1-6;

Provided, however, that if a federal, state, or local law enforcement agency determines that any notice required under this Provision would interfere with an ongoing investigation, the notice can be delayed upon the written request of the law enforcement agency for a specified period that the law enforcement agency determines is reasonably necessary. A law enforcement agency may, by a subsequent written request, revoke such delay as of a specified date or extend the period set forth in the original request to a specified date if further delay is necessary.

VII. Covered Incident Reports to the Commission

IT IS FURTHER ORDERED that, within ten (10) days of any notification to a United States federal, state, or local entity of a Covered Incident, Respondents must submit a report to the Commission. The report must include, to the extent possible:

A. The date, estimated date, or estimated date range when the Covered Incident occurred;

B. A description of the facts relating to the Covered Incident, including the causes of the Covered Incident, if known;

C. A description of each type of information that was affected by the Covered Incident;

D. The number of consumers whose information was affected by the Covered Incident;

E. The acts that Respondents have taken to date to remediate the Covered Incident and protect Personal Information from further exposure, acquisition, or access, and protect affected individuals from identity theft or other harm that may result from the Covered Incident;

F. As applicable, a statement that Respondents have received a request from a federal, state, or local law enforcement agency to delay notice to Future Affected Consumers and Facilities on the basis that such notice would interfere with an ongoing investigation and a copy of such request; and

G. A representative copy of any materially different notice Respondents will send or have sent to consumers or to any United States federal, state, or local government entity.

Unless otherwise directed by a Commission representative in writing, all Covered Incident reports to the Commission pursuant to this Order must be emailed to DEbrief@ftc.gov or sent by overnight courier (not the U.S. Postal Service) to: Associate Director for Enforcement, Bureau of Consumer Protection, Federal Trade Commission, 600 Pennsylvania Avenue NW, Washington, DC 20580. The subject line must begin: "In re Global Tel*Link Corporation, FTC File No. 2123012."

VIII. Prohibition Against Misrepresentations About Security and Privacy

IT IS FURTHER ORDERED that Respondents, and Respondents' officers, agents, employees, and attorneys, and all other persons in active concert or participation with any of them, who receive actual notice of this Order, whether acting directly or indirectly, in connection with promoting or offering for sale any product or service must not misrepresent in any manner, expressly or by implication:

A. Respondents' privacy and security measures to prevent unauthorized access to Personal Information;

B. 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;

C. The extent to which Respondents have notified or will notify affected parties in connection with a Covered Incident;

D. The extent to which Respondents meet or exceed industry-standard security or privacy practices; and

E. The extent to which Respondents otherwise protect the privacy, security, availability, confidentiality, or integrity of Personal Information.

IX. Notification to Consumers Affected by the Identified Breach

IT IS FURTHER ORDERED that, within one hundred and twenty (120) days of Telmate receiving approval of the Third Party from the Associate Director for Enforcement for the Bureau of Consumer Protection pursuant to Provision V of this Order entitled "Credit Monitoring and Identity Protection Product":

A. Respondents must post Clearly and Conspicuously on the home page of each of Respondents' websites and the home screen of each of Respondents' mobile applications that has been used to provide Telmate products and services an exact copy of the notice attached hereto as Attachment A ("Banner Notice"), including a hyperlink to an exact copy of the notice attached hereto as Attachment B ("Website and App Notice"). Respondents must leave these Notices in place for one year after posting them. Respondents must not include with the Website and App Notice any other information, documents, or attachments; and

B. Telmate and its successors and assigns must provide a notice to each Affected Consumer to whom Respondents did not send written notice of the Identified Breach in May of 2021. The notice must consist solely of an exact copy of the notice attached hereto as Attachment C ("Direct Notice"). Respondents must not include with the Direct Notice any other information, documents, or attachments apart from those provided by the Third

Party for credit monitoring enrollment.

X. Notification to Facilities

IT IS FURTHER ORDERED that, within one hundred and twenty (120) days of approval of the Third Party offering, providing, and maintaining the Product pursuant to the Provision of this Order entitled "Credit Monitoring and Identity Protection Product," Telmate and its successors and assigns must provide a notice to all Facilities with a known, present relationship to one or more incarcerated Affected Consumers. The notice must describe Telmate and its successors and assigns' obligations under the Provisions of this Order entitled "Notification to Consumers Affected by the Identified Breach" and "Credit Monitoring and Identity Protection Product," including:

A. All information necessary for the Facility to facilitate incarcerated Affected Consumers' ability to receive communications required pursuant to this Order and to communicate with the Third Party;

B. The identity of and contact information for the Third Party; and

C. Information regarding how the costs of incarcerated Affected Consumers' communications with the Third Party are to be billed or covered.

Such notice must be sent by first-class mail, postage paid and return receipt requested, or by courier service with signature proof of delivery.

XI. Acknowledgments of the Order

IT IS FURTHER ORDERED that Respondents obtain acknowledgments of receipt of this Order:

A. Each Respondent, within ten (10) days after the effective date of this Order, must submit to the Commission an acknowledgment of receipt of this Order sworn under penalty of perjury.

B. Each Respondent must deliver a copy of this Order to: (1) all principals, officers, directors, and LLC managers and members; (2) all employees having managerial responsibilities for conduct related to the subject matter of the Order and all agents and representatives who participate in conduct related to the subject matter of the Order; (3) each business that Respondents control, directly or indirectly; and (3) any business entity resulting from any change in structure as set forth in the Provision titled Compliance Reports and Notices. Delivery must occur within ten (10) days after the effective date of this Order for current personnel. For all others, delivery must occur before they assume their responsibilities.

C. From each individual or entity to which a Respondent delivered a copy of this Order, that Respondent must obtain, within thirty (30) days, a signed and dated acknowledgment of

receipt of this Order.

XII. Compliance Reports and Notices

IT IS FURTHER ORDERED that Respondents make timely submissions to the Commission:

A. One (1) year after the issuance date of this Order, each Respondent must submit a compliance report, sworn under penalty of perjury, in which each Respondent must:

1. Identify the primary physical, postal, and email address and telephone number, as designated points of contact, which representatives of the Commission, may use to communicate with Respondent;

2. Identify all of that Respondent's businesses by all of their names, telephone numbers, and physical, postal, email, and Internet addresses;

3. Describe the activities of each business, including the goods and services offered; each means by which consumers can access each business's goods and services, including each website or mobile application that consumers can use to access each service; the extent to which consumers can or must register or create an account or profile in order to access goods or services; the types of Personal Information that Respondents collect in connection with consumers' use of goods or services, and the extent to which Respondents disclose any of that information to Facilities; the means of advertising, marketing, and sales; and the involvement of any other Respondent;

4. Describe in detail whether and how that Respondent is in compliance with each Provision of this Order, including a discussion of all of the changes the Respondent made to comply with the Order; and

5. Provide a copy of each Acknowledgment of the Order obtained pursuant to this Order, unless previously submitted to the Commission.

B. Each Respondent must submit a compliance notice, sworn under penalty of perjury, within fourteen (14) days of any change in the following:

1. Any designated point of contact; or

2. The structure of any Respondent or any entity that Respondent has any ownership interest in or controls directly or indirectly that may affect compliance obligations arising under this Order, including: creation, merger, sale, or dissolution of the entity or any subsidiary, parent, or affiliate that engages in any acts or practices subject to this Order.

C. Each Respondent must submit notice of the filing of any bankruptcy petition, insolvency proceeding, or similar proceeding by or against such Respondent within fourteen (14) days of its filing.

D. Any submission to the Commission required by this Order to be sworn under penalty of perjury must be true and accurate and comply with 28 U.S.C. § 1746, such as by concluding: "I declare under penalty of perjury under the laws of the United States of America that the foregoing is true and correct. Executed on: _____" and supplying the date, signatory's full name, title (if applicable), and signature.

E. Unless otherwise directed by a Commission representative in writing, all submissions to the Commission pursuant to this Order must be emailed to DEbrief@ftc.gov or sent by overnight courier (not the U.S. Postal Service) to: Associate Director for Enforcement, Bureau of Consumer Protection, Federal Trade Commission, 600 Pennsylvania Avenue NW, Washington, DC 20580. The subject line must begin: "In re Global Tel*Link Corporation, FTC File No. 2123012."

XIII. Recordkeeping

IT IS FURTHER ORDERED that Respondents must create certain records and retain each such record for five (5) years, unless otherwise specified below. Specifically, each Respondent must create and retain the following records:

A. Accounting records showing the revenues from all goods or services sold, the costs incurred in generating those revenues, and resulting net profit or loss;

B. Personnel records showing, for each person providing services in relation to any aspect of the Order, whether as an employee or otherwise, that person's: name; addresses; telephone numbers; job title or position; dates of service; and (if applicable) the reason for termination;

C. Copies or records of all consumer complaints concerning the subject matter of the Order, whether received directly or indirectly, such as through a third party, and any response;

D. A copy of each unique advertisement, marketing or business proposal (including any response to a Request for Proposal), or other marketing material making a representation subject to this Order;

E. A copy of each widely disseminated representation by Respondents that relates to any Covered Incident or describes the extent to which Respondents maintain or protect the privacy, security and confidentiality of any Personal Information, including any representation concerning a change in any website or other service controlled by Respondents that relates to the privacy, security, and confidentiality of Personal Information;

F. For five (5) years after the date of preparation of each Assessment required by this Order, all materials relied upon to prepare the Assessment, whether prepared by or on behalf of Respondents, including all plans, reports, studies, reviews, audits, audit trails, policies, training materials, and Assessments, and any other materials concerning Respondents' compliance with related Provisions of this Order, for the compliance period covered by such Assessment;

G. For five (5) years from the date received, copies of all subpoenas and other communications with law enforcement, if such communication relate to Respondents' compliance with this Order or relate to any Covered Incident;

H. All records necessary to demonstrate full compliance with each provision of this Order, including all submissions to the Commission.

XIV. Compliance Monitoring

IT IS FURTHER ORDERED that, for the purpose of monitoring Respondents' compliance with this Order:

A. Within ten (10) days of receipt of a written request from a representative of the Commission, each Respondent must: submit additional compliance reports or other requested information, which must be sworn under penalty of perjury, and produce records for inspection and copying.

B. For matters concerning this Order, representatives of the Commission are authorized to communicate directly with each Respondent. Respondents must permit representatives of the Commission to interview anyone affiliated with any Respondent who has agreed to such an interview. The interviewee may have counsel present.

C. The Commission may use all other lawful means, including posing through its representatives as consumers, suppliers, or other individuals or entities, to Respondents or any individual or entity affiliated with Respondents, without the necessity of identification or prior notice. Nothing in this Order limits the Commission's lawful use of compulsory process, pursuant to Sections 9 and 20 of the FTC Act, 15 U.S.C. §§ 49, 57b-1.

XV. Order Effective Dates

IT IS FURTHER ORDERED that this Order is final and effective upon the date of its publication on the Commission's website (ftc.gov) as a final order. This Order will terminate 20 years from the date of its issuance (which date may be stated at the end of this Order, near the Commission's seal), or 20 years from the most recent date that the United States or the Commission files a complaint (with or without an accompanying settlement) in federal court alleging any violation of this Order, whichever comes later; *provided*, *however*, that the filing of such a complaint will not affect the duration of:

A. Any Provision in this Order that terminates in less than 20 years;

B. This Order's application to any Respondent that is not named as a defendant in such complaint; and

C. This Order if such complaint is filed after the Order has terminated pursuant to this Provision.

Provided, further, that if such complaint is dismissed or a federal court rules that the Respondent did not violate any provision of the Order, and the dismissal or ruling is either not appealed or upheld on appeal, then the Order will terminate according to this Provision as though the complaint had never been filed, except that the Order will not terminate between the date such complaint is filed and the later of the deadline for appealing such dismissal or ruling and the date such dismissal or ruling is upheld on appeal.

By the Commission.

April J. Tabor
Secretary

SEAL:
ISSUED: February 23, 2024