212-3012

UNITED STATES OF AMERICA
BEFORE THE FEDERAL TRADE COMMISSION

COMMISSIONERS: **Lina 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.**	**DOCKET NO.**

COMPLAINT

The Federal Trade Commission, having reason to believe that Global Tel*Link Corporation, a corporation, doing business as GTL, also doing business as ViaPath Technologies; Telmate, LLC, a limited liability company, also doing business as ViaPath Technologies; and TouchPay Holdings, LLC, a limited liability company, also doing business as GTL Financial Services (collectively, "Respondents"), have violated the provisions of the Federal Trade Commission Act, and it appearing to the Commission that this proceeding is in the public interest, alleges:

1. 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.

2. 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.

3. 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.

4. Respondents offer various products and services to jails, prisons, and detention facilities, to individual consumers incarcerated in these facilities, and to family, friends and other contacts of incarcerated consumers.

5. These products and services include communications services for incarcerated individuals to correspond with their non-incarcerated contacts, and payment services to provide incarcerated individuals with access to funds. Through these services, Respondents collect a significant amount of sensitive information from incarcerated individuals and their contacts, such as their names, addresses, passport numbers, driver's license numbers, Social Security numbers, and financial account information.

6. Respondents have made numerous promises to protect the sensitive personally identifiable information that they collect in connection with offering their products and services. However, as alleged below, Respondents failed to employ reasonable data security safeguards to protect this information. This failure resulted in a security incident that exposed hundreds of thousands of consumers' information. Respondents then failed to provide timely notice to affected consumers so that they could take steps to protect themselves from identity theft. In addition, Respondents also made multiple misleading representations about the data security incident. Respondents' data security failures constitute deceptive and unfair practices in violation of Section 5(a) of the FTC Act.

7. Respondents have operated as a common enterprise while engaging in the unlawful acts and practices alleged below. Respondents have conducted the business practices described below through an interrelated network of companies that have, among other things, common ownership and control, common officers and managers, shared office locations, shared resources, and unified advertising. Because Respondents have operated as a common enterprise, each of them is jointly and severally liable for the acts and practices alleged below.

8. The acts and practices of Respondents alleged in this complaint have been in or affecting commerce, as "commerce" is defined in Section 4 of the Federal Trade Commission Act.

Respondents' Business Practices

9. Respondents contract with state Departments of Corrections, the Federal Bureau of Prisons, county and city jails, immigration detention facilities, and juvenile detention facilities (collectively, "Facilities") to provide certain products and services to those Facilities, individuals incarcerated therein, and incarcerated individuals' outside contacts. Respondents have contracted with public and private Facilities located in all 50 states, the District of Columbia, and Puerto Rico.

10. Individual users of Respondents' products and services include people who are incarcerated in the Facilities. In marketing materials, Respondents have touted that more than 1.9 million incarcerated people, constituting "more than 85% of the U.S. inmate population," use GTL's services. These individuals include both people who have been convicted of crimes and are incarcerated in prisons and people, such as those held in jails in pre-trial detention, who have not been convicted of any crime. Additionally, in 2020, Respondents' services were used by

over 13 million consumers who were not incarcerated (e.g., family and friends of incarcerated people). GTL's annual net revenue is over $600 million.

11. The precise products and services provided, and the costs of those products and services for individual consumers, vary by Facility. If a Facility chooses to engage Respondents' services, Respondents often require by contract that they be the sole providers of those products and services within that given Facility. Therefore, incarcerated consumers and their outside contacts frequently do not have the option of choosing an alternative provider.

12. Incarcerated consumers access Respondents' products and services using tablets and kiosks that are provided by Respondents and are available within Facilities. Consumers who are not incarcerated can access Respondents' services through Respondents' websites and mobile applications, including www.getttingout.com and the GettingOut mobile applications (collectively, "GettingOut") and web.connectnetwork.com and the ConnectNetwork mobile applications (collectively, "ConnectNetwork").

13. Once a consumer has created an account on GettingOut or ConnectNetwork, the consumer can use the same account to access products and services available through either brand. For example, consumers who have registered with GettingOut can use GettingOut or ConnectNetwork to communicate with incarcerated individuals using voice calls, video calls, or written messages similar to text messages or e-mail. They can also use GettingOut or ConnectNetwork to make financial deposits to an incarcerated person's inmate trust account, allowing the incarcerated individual to use the funds for various purposes including purchasing items from Facility commissaries, posting bail, and paying fees or fines.

14. Respondents charge incarcerated consumers and their non-incarcerated contacts to use these services. These charges vary based on the services used and are established in Respondents' contracts with Facilities. For example, to use their communications services, Respondents have charged consumers rates such as $0.18-0.25 per minute to make a voice call, $0.25 per minute to make a video call, $1.00 to leave a voicemail message, $0.25 to send a written message, and $0.25-0.50 for each photo or video attachment to a written message. To use their payments services to make a deposit, Respondents have in many instances charged consumers between $2.95 and $11.50 plus 3.5% of the deposit amount.

15. To create an account to use Respondents' services, incarcerated consumers and their contacts are required to provide Respondents with certain personal information, including, in many cases, their names, addresses, government identification numbers such as passport numbers or driver's license numbers, Social Security numbers, and financial account information.

16. Using the significant volume of information Respondents collect from incarcerated individuals and their contacts, Respondents also offer products and services that allow Facilities to surveil and investigate incarcerated consumers and their non-incarcerated contacts.

Data Security Promises

17. Respondents have made and continue to make various representations regarding their information security capabilities and practices. For example, Respondents market themselves to Facilities as an organization that is "security-focused from the inside out," and that their "attention is focused on…security," specifically "preventing data breaches and hacks."

18. Since 2017, Respondents have disseminated a YouTube video highlighting the importance of data security in Respondents' industry. The video features GTL executives making the following statements:

a. "GTL is different in data security from our competition" and data security is "the cornerstone of what we do."

b. Data security is important for Respondents' business because incarcerated users use Respondents' services to "shar[e] confidential information," including information related to commissary services, medical services, and phone services.

c. "A facility that's looking for a secure environment…should be asking those questions: have you had a breach? And if you've had one, what have you done to correct it?"

19. In seeking new or continued business from current and potential Facility customers, Respondents regularly respond to those Facilities' Requests for Proposals ("RFPs"). In numerous instances, as part of the RFP process, Facilities have requested information about Respondents' data security practices.

20. Since May 2017, as part of their RFP responses to Facilities seeking information about Respondents' data security practices, Respondents have disseminated or caused to be disseminated a marketing document entitled "Information Security Framework." This document states: "At GTL, we take information security and data protection very seriously. That's why we've gone to exceptional lengths to safeguard each customer's data and private information that is generated through the course of their relationship with us. Our security architecture provides our customers the reassurance that their data won't fall into the wrong hands."

21. The "Information Security Framework" document goes on to make the following statements regarding Respondents' use of specific data security safeguards:

a. "[C]ontrols are in place to limit access only from specific IP addresses. This means that access to customer data will be denied if a request is from an unknown IP address."

b. "[M]ultiple layers of 128-bit encryption and perimeter firewall protection prevent unauthorized access from the Internet."

c. "A robust centralized log monitoring solution provides alerts to the GTL Information Security Department based on predefined and internally developed alarm rules. This application is monitored to detect other anomalies that might indicate inappropriate use of GTL assets….GTL uses industry accepted log monitoring so[ft]ware to perform file integrity monitoring and to provide real time monitoring of application, security, and system event logs. Using this log monitoring so[ft]ware, the GTL Information Security Department monitors log events 24/7 and investigates all alerts."

d. "[A]ny changes to firewall hardware or so[ft]ware or security rules are approved by GTL's Information Security Department, follow all change control policies and procedures, and are properly documented."

e. "Intrusion Prevention Systems are deployed to alert the GTL Information Security Department to potential attacks and automatically block such attacks. Many companies choose to rely on an Intrusion Detection System that simply alerts of potential attacks, but GTL's systems automatically block suspected malicious traffic."

22. Since May 2017, in response to RFPs from potential Facility customers, Respondents have also disseminated or caused to be disseminated a marketing document entitled "Solution Integration." This document states: "Our integrated solutions also help enhance data and technology security. We follow security best practices, the latest encryption methodologies, and proper protocols to ensure our system offers the most robust data and wireless security in the market. Our technologies leverage multiple layers of firewalls, SSL, and best-in-industry security standards to ensure all data transmitted through our systems are secure."

23. Respondents have also made security representations to individual consumers. Since at least January 2020, Respondents have disseminated privacy policies on their public-facing websites, including on the GettingOut website. These privacy policies have made and continue to make the following representation: "We seek to use industry standard physical, technical and administrative security measures designed to protect your personally identifiable information. However, no data transmission or storage system can be guaranteed to be 100% secure. If you have reason to believe that your interaction with us is no longer secure (for example, if you feel that the security of any account you might have with us has been compromised), please immediately notify us in accordance with the 'Contact Us' section above."

The Test Environment and Respondents' Data Security Practices

24. In operating and providing some of their products and services, Respondents rely on search and storage software ("Search Software"). In 2019, Respondents initiated a process to transition to a newer version of the Search Software.

25. The engineers working to plan and execute the Search Software update included employees of a third-party vendor (the "Vendor") with which Respondents contract to provide software development and other services. Respondents' employees supervised the day-to-day

activities of engineers working on the Search Software update, including those employed by the Vendor.

26. In or about August 2020, Respondents copied a large volume of production data (i.e., real data from and about users of Respondents' products and services) into an Amazon Web Services ("AWS") cloud storage environment (the "Test Environment") for the purpose of testing the new Search Software version.

27. As discussed in further detail in Paragraph 31, the data copied to the Test Environment included personally identifiable information pertaining to numerous incarcerated, non-incarcerated, and Facility users of Respondents' products and services, including communications services used by incarcerated consumers and their contacts and monitoring services used by Facilities.

28. Though the Test Environment contained personally identifiable information, Respondents failed to provide reasonable security for that information. Among other things:

a. Respondents did not take any steps to encrypt or otherwise obfuscate the data that they transferred to the Test Environment, but rather stored consumers' sensitive, personally identifiable information in clear, readable text;

b. Respondents did not use automated monitoring software on the Test Environment, including free AWS features that would have generated alerts if the security settings of the Test Environment were changed;

c. Respondents did not employ a perimeter firewall to protect the Test Environment;

d. Respondents did not employ a log monitoring solution that provided alerts to the GTL Information Security Department to protect the Test Environment;

e. Respondents did not employ an Intrusion Prevention System to protect the Test Environment;

f. Though the Vendor had access to highly sensitive personally identifiable information held within Respondents' systems, including the Test Environment, Respondents took no steps to vet or assess the Vendor's data security practices;

g. Respondents also did not provide, or require the Vendor to provide, the Vendor's engineers with secure development training or with other data security training appropriate to their job duties; and

h. Respondents did not take reasonable steps to inventory or track consumers' personally identifiable information, including tracking which consumers' personally identifiable information was transferred and the categories of personally identifiable information that they transferred to the Test Environment.

The Incident

29. On or about August 11, 2020, a technician employed by the Vendor changed the security settings of the Test Environment. As a result of this change, from at least August 11, 2020 to August 13, 2020, the Test Environment was left accessible via the internet without password protection or other access controls to prevent unauthorized persons from accessing and exfiltrating data from the Environment ("Incident").

30. Approximately 649,500 unique individuals' personally identifiable information was contained within the Test Environment at the time of the Incident.

31. This personally identifiable information included individuals' full names; dates of birth; phone numbers; usernames or email addresses in combination with passwords; home addresses; driver's license numbers; passport numbers; location information; information about individuals' race, religion, and whether they are transgender; approximately 80,000 grievances submitted by incarcerated consumers to Facilities; and the content, dates and times, senders, and recipients of approximately 75,000 written messages that incarcerated and non-incarcerated users had exchanged using Respondents' services. In numerous instances, the written messages contained payment card numbers, financial account information, and Social Security numbers.

32. The Test Environment also contained a database of deposit information, including data fields such as "account_posted_at," "amount," "card_owner_name," "deposit_type," and "dest_account_id."

33. Beginning on or about August 12, 2020, there were multiple instances of access to the Test Environment from IP addresses not associated with Respondents. Unidentified individuals accessing the Test Environment from those IP addresses accessed approximately 44,000,000,000 bytes of data stored in the Test Environment. Forensic analysis conducted by or on behalf of Respondents has indicated that there was exfiltration of data from the Test Environment by one or more of these individuals.

34. Respondents learned of the Incident on August 13, 2020, when a security researcher contacted Respondents and stated that he had discovered "an unprotected, publicly available database instance which seems to be part of GTL / Telmate cloud infrastructure and contains non-public information, such as inmates[’] personal details, emails, auth history, messages and much more." After confirming the researcher's findings, Respondents reconfigured the Test Environment so that it was no longer accessible from the internet.

35. On September 1, 2020, Respondents received a message from a company that provides identity monitoring services to consumers stating that the company's engineers "believe[d] they [had] come across sensitive data related to GTL." Following this communication, Respondents worked with the identity monitoring company to retrieve copies of data that had been released on the "dark web," i.e., on websites that are used to buy and sell illicitly obtained data for use in connection with fraud, identity theft, and other criminal purposes. Subsequent data analysis suggested that the data provided by the identity monitoring company aligned with data believed to have been impacted in the Incident.

36. As early as November 2020, Respondents received multiple complaints from consumers stating that the consumers' personally identifiable information obtained from Respondents had been located on the dark web. This personally identifiable information included names, addresses, phone numbers, dates of birth, and driver's license issue states. Some consumer complaints also indicated that consumers had been alerted to fraudulent transactions on their credit cards following the Incident.

37. In part as a result of Respondents' data security failures, hundreds of thousands of consumers' personally identifiable information was exposed to the internet, was exfiltrated by unauthorized individuals, and was made available on the dark web. These failures resulted in financial injury to consumers, including because consumers experienced unauthorized payment card activity shortly after learning of the Incident from third-party credit monitoring services. Additionally, the public exposure of consumers' communications with loved ones and sensitive information contained in grievance forms is, at a minimum, a serious invasion of privacy that may cause them stigma, embarrassment, and/or emotional distress. In some cases, that information, like consumers' location information and whether individuals identify as transgender, has concerning implications for consumers' safety.

Misrepresentations to Consumers Regarding the Incident and Failure to Notify Consumers

38. On September 4, 2020, Comparitech, a data privacy and security blog, published an article about the Incident. Comparitech's article contains the following statement, which Respondents had provided to Comparitech on September 3, 2020 via e-mail:

> Telmate, a GTL subsidiary immediately locked down the server as a precaution upon being made aware of a vulnerability in the data system due to the actions of one of our vendors. This vulnerability was swiftly corrected, the data security team was immediately supplemented with the assistance of third-party consultants and we continue to work closely with law enforcement authorities as we conduct further inquiry into this incident. *Based on the current facts of the investigation, no medical data, passwords, or consumer payment information were affected. We continue to speak with and notify necessary parties, including the affected Telmate customers – a small subset of all GTL customers – about the incident and the actions we have taken to safeguard data.* The security of the data we keep is of the utmost importance to us, and we are committed to doing everything we can to keep it safe. (Emphasis added.)

39. Respondents' statement to Comparitech was false or misleading. Among other reasons, the statement was false or misleading as to the severity of the Incident and the risk to individual consumers, because:

a. Respondents stated that their investigation to date had not indicated that medical data or payment information was affected, but in fact Respondents knew at least as of August 19, 2020 that some credit card numbers and medical information, including

incarcerated consumers' requests to see medical staff, were included in information affected by the Incident;

b. Respondents' statement failed to disclose additional categories of sensitive personally identifiable information that were affected or potentially affected by the Incident, including addresses, email addresses, Social Security numbers, passport numbers, and driver's license numbers; and

c. Respondents stated that "we continue to speak with and notify necessary parties, including the affected Telmate customers," but, in fact, Respondents did not contact any affected individuals to notify them of the Incident until May 2021.

40. In or about May 2021, Respondents notified approximately 45,000 individual users that their personally identifiable information had been exposed as a result of the Incident. To date, Respondents have provided no notice to the potentially hundreds of thousands of additional users whose information was contained in the Test Environment at the time of the Incident and therefore may have been exposed.

41. Because Respondents delayed notifying individual users that their personally identifiable information had been or could have been affected by the Incident for approximately nine months, those users did not have an opportunity to take actions to protect themselves from identity theft, such as by implementing a credit freeze.

Misrepresentations to Facilities Regarding the Incident

42. Additionally, on multiple occasions since the Incident, in connection with responding to RFPs by prospective Facility customers, Respondents have represented that Respondents have never experienced a data security breach or had not experienced a data security breach within a particular time frame that includes the dates of the Incident.

43. For example, since December 2020, Respondents have stated in their RFP responses to potential Facility customers that "there were no system incidents that resulted in a significant failure in the achievement of one or more of service commitments and system requirements throughout the period April 1, 2020, to September 30, 2020," where "system requirements" are defined to include that "Logical access to programs, data and computer resources is restricted to authorized and appropriate users, and such users are restricted to performing authorized and appropriate actions."

44. In other instances, Respondents have submitted RFP responses stating that, e.g., Respondents have never experienced a data security breach or have not experienced a data security breach within the past five years.

Count I
Unfair Data Security Practices

45. As described in Paragraph 28, Respondents failed to employ reasonable and appropriate measures to protect consumers' personally identifiable information.

46. This failure caused or was likely to cause substantial injury to consumers that is not outweighed by countervailing benefits to consumers or competition and is not reasonably avoidable by consumers themselves. This practice is an unfair act or practice.

Count II
Unfair Failure to Notify Affected Consumers of the Incident

47. As described in Paragraphs 38-40, Respondents failed to timely notify affected consumers that their personally identifiable information had been exposed as a result of the Incident.

48. This failure caused or is likely to cause substantial injury to consumers that is not outweighed by countervailing benefits to consumers or competition and is not reasonably avoidable by consumers themselves. This practice is an unfair act or practice.

Count III
Misrepresentations Regarding Data Security

49. As described in Paragraphs 17-23, in connection with the advertising, promotion, offering for sale, or sale of communications and payment services, Respondents have represented, directly or indirectly, expressly or by implication, that they implemented reasonable and appropriate measures to protect personally identifiable information against unauthorized access.

50. In fact, as described in Paragraph 28, Respondents did not implement reasonable and appropriate measures to protect personally identifiable information in the Test Environment against unauthorized access. Therefore, the representation set forth in Paragraph 49 is false or misleading.

Count IV
Misrepresentations to Individual Users Regarding the Incident

51. As described in Paragraph 38, in connection with the advertising, promotion, offering for sale, or sale of communications and payment services, Respondents represented, directly or indirectly, expressly or by implication, that they had no reason to believe that consumers' sensitive personally identifiable information was affected by the Incident.

52. In fact, as described in Paragraph 39, Respondents had reason to believe that consumers' sensitive personally identifiable information was affected by the Incident. Therefore, the representation set out in Paragraph 51 was false or misleading.

Count V
Misrepresentations to Individual Users
Regarding Notice

53. As described in Paragraph 38, in connection with the advertising, promotion, offering for sale, or sale of communications and payment services, Respondents represented that they would timely notify users whose personally identifiable information had been exposed as a result of the Incident.

54. In fact, as described in Paragraphs 39-41, Respondents failed to provide timely notice to users whose personally identifiable information was exposed because of the incident. Therefore, the representation set out in Paragraph 53 was false or misleading.

Count VI
Deceptive Representations to Facilities Regarding the Incident

55. As described in Paragraphs 42-44 in connection with the advertising, promotion, offering for sale, or sale of communications and payment services, in multiple instances since the Incident, Respondents have represented to Facilities that they have never experienced a data security breach or that they had not experienced a data security breach within a particular timeframe that includes the dates of the Incident.

56. In fact, as described in Paragraphs 29-37, the representations set out in Paragraph 55 have been false or misleading.

Violations of Section 5

57. The acts and practices of Respondents as alleged in this complaint constitute unfair or deceptive acts or practices in or affecting commerce in violation of Section 5(a) of the Federal Trade Commission Act.

THEREFORE, the Federal Trade Commission this _____ day of _____, 2023, has issued this Complaint against Respondents.

By the Commission.

April J. Tabor
Secretary

SEAL: