TIO Networks
2211 N 1st St.
San Jose, CA 95131

October 23, 2018

BY U.S. MAIL

Office of the Attorney General
33 Capitol Street
Concord, NH 03301

To Whom It May Concern:

This letter supplements our letter dated December 22, 2017, which provided formal notice of a computer data security incident, consistent with N.H. Rev. Stat. Ann. § 359-C:20, and our letter dated February 2, 2018.

We have not discovered proof that any particular individual's data was accessed, acquired, or misused. As noted in our December 22 and February 2 letters, TIO has notified your office, and potentially affected individuals, out of an abundance of caution because the servers involved in this incident stored data such as customer names, contact information, and subscriber/billing account numbers. The TIO systems also stored personal information such as payment card information, bank account information, Social Security and other government identification numbers, and account usernames and passwords.

Since sending the February 2 letter, TIO has continued to work assiduously to review the data contained on TIO's systems, communicate with impacted billers and other non-biller entities associated with potentially impacted individuals, and send notices to potentially affected individuals. Based on the information available to TIO to date, we believe there are approximately 11 additional potentially affected individuals who reside in your state who were associated with entities that have permitted TIO to notify individuals, in addition to the approximately 330[1] individuals who we previously

[1] This revised estimate accounts for additional analysis, including de-duping, we performed since our February letter.

identified and reported to your office. We do not anticipate that we will identify further affected individuals.

The attached appendix identifies each biller or non-biller entity that permitted TIO to notify potentially affected individuals; the approximate number of individuals associated with that biller or non-biller entity whose information may have been affected; and the potentially affected personal information for those individuals. By October 23, 2018, TIO expects to have notified approximately 11 residents of your state through mail and/or email, in addition to the 330 residents notified by TIO or directly by billers that informed TIO of their notification efforts. As we do not anticipate identifying any additional potentially affected individuals, we now believe that all potentially affected residents in your state who TIO was permitted to notify have been notified.

As we hope our efforts to date have made clear, TIO is committed to mitigating the impact of this incident and to answering any questions that consumers in your state and members of your office may have. Please feel free to contact me with any questions at (415) 777-4800.

Respectfully yours,

/s/ John Kunze

John Kunze
President
TIO Networks USA, Inc.

Enclosures

Schedule

Name of Biller or Other Entity Associated with Potentially Impacted Individuals	Alliance Data (Comenity Bank)
Contact Information	Alliance Data (Comenity Bank) 3075 Loyalty Circle Columbus, OH 43219 Ann B. Zallocco Director & Counsel, Law Department 614 944-5804 Ann.Zallocco@alliancedata.com
Estimated Number of Individuals with Potentially Affected Personal Information in this Jurisdiction	4
Date of Consumer Notification	Began week of 5/18/2018
Form of Individual Consumer Notification	Mail
Potentially Affected Personal Information	Payment Card Information

Schedule

Name of Biller or Other Entity Associated with Potentially Impacted Individuals	Florida Power & Light Company
Contact Information	Florida Power & Light Company 700 Universe Blvd. Juno Beach, FL 33408 Rachel Budke, Esq. (561) 304-5209 Rachel.Budke@fpl.com
Total Estimated Number of Individuals with Potentially Affected Personal Information in this Jurisdiction	83 (As of 10/23/2018)
Estimated Number of Individuals with Potentially Affected Personal Information in this Jurisdiction who were Identified After the February 2, 2018 Letter	1
Date of Consumer Notification	Began week of 12/11/2017
Form of Individual Consumer Notification	Mail
Potentially Affected Personal Information	Bank Account Information

Schedule

Name of Biller or Other Entity Associated with Potentially Impacted Individuals	TIO (TIO Agents)
Contact Information	Jim Pastore Debevoise & Plimpton LLP 919 Third Ave. New York, NY 10022 (212) 909-6793 jjpastore@debevoise.com
Total Estimated Number of Individuals with Potentially Affected Personal Information in this Jurisdiction	38 (As of 10/23/2018)
Estimated Number of Individuals with Potentially Affected Personal Information in this Jurisdiction who were Identified After the February 2, 2018 Letter	6
Date of Consumer Notification	Began week of 12/18/2017
Form of Individual Consumer Notification	Mail
Potentially Affected Personal Information	Social Security Number

Return Mail Processing
PO Box 51484
Livonia, MI 48151-5484

[DATE]

P1IWKN00100001 - 194246692
[CUSTOMER NAME]
[STREET ADDRESS]
[TOWN, STATE, ZIP]

NOTICE OF DATA BREACH

Dear [CUSTOMER NAME],

I am writing to let you know about an incident involving data housed on the systems of TIO Networks USA, Inc. and its affiliates, including Softgate Systems; Inc., Softgate Systems of California, Inc.; and Global Express Money Orders, Inc. ("TIO"). TIO provides technology that helps customers pay bills through self-service kiosks, at retail locations, and through mobile and web applications.

I've Never Heard Of TIO – Why Am I Receiving This?

TIO's services are used by some of the companies that provide you services – like your utility company or telecom company – so you might not know that the company is using TIO. When you pay for services, TIO makes sure your payment gets to the company. Our records indicate that you used TIO's services when you paid:

[BILLER NAME]

[BILLER ADDRESS]

What Happened?

TIO Networks was acquired by PayPal Holdings, Inc. ("PayPal") on July 18, 2017. On November 10, TIO's operations were suspended after the discovery of security vulnerabilities in its systems. The investigation to date has uncovered evidence of unauthorized access to the TIO network, including locations that stored personal information of some of TIO's customers and customers of the companies that TIO services. We have no proof, however, that your data was accessed, acquired, or misused. The PayPal platform, which is separate from the TIO network, is not impacted by this situation in any way and PayPal's customers' data remains secure.

What Information Was Involved?

Although we have no proof that your data was accessed, acquired, or misused, we are notifying you in an abundance of caution because the TIO servers involved in this incident stored data such as customer names, contact information, and subscriber/billing account numbers. The TIO systems also stored personal information such as payment card information, bank account information, Social Security and other government identification numbers, and account usernames and passwords. With respect to the company you did business with, the TIO servers stored the following personal information:

[POTENTIALLY AFFECTED PERSONAL INFORMATION]

Our evidence of the earliest possible date of intrusion dates back to at least 2014, and data on TIO's systems prior to that date may have been affected. We continue to investigate the earliest evidence of unauthorized access.

What We Are Doing

We sincerely regret this incident and are working hard to protect you and your personal information. In addition to suspending its services, TIO contacted the appropriate law enforcement and other authorities, and has brought in outside cybersecurity experts to investigate.

We are also providing you with one year of complimentary identity protection that includes credit monitoring, identity theft insurance, and assistance with combating identity theft and fraud, should any be detected.

Visit **www.experianidworks.com/creditone** to activate and take advantage of your identity protection.

*You have until **March 31, 2018** to activate your identity protection.*

Activation Code: [XXXXXXXX]

To activate your membership by phone instead of online, please call 1-855-272-6796. Be prepared to provide engagement number [XXXXXXX].

What You Can Do

I am enclosing additional steps that you can take to protect yourself, including how to place a fraud alert or a security freeze on your credit file with the three major credit reporting agencies. In addition, if you have an online account with TIO, you should consider resetting the password for the account (and for any other accounts for which you use the same password).

For More Information

We sincerely regret any inconvenience this incident may cause you. For the latest information, please visit www.tio.com. You can also contact us in writing at 2211 N 1st St, San Jose, CA 95131, or by phone at 1-855-272-6796.

Para ayuda en español, por favor visitar www.tio.com.

Sincerely,

John Kunze
President
Tio Networks USA, Inc.

ADDITIONAL RESOURCES

You should remain vigilant for instances of fraud or identity theft by reviewing your account statements and closely monitoring your credit reports, which are available to you free of charge. You may obtain a free copy of your credit report once every 12 months from each of the three nationwide credit reporting agencies. Contact information for these agencies is as follows:

Equifax: P.O. Box 740241, Atlanta, GA 30374, www.equifax.com, 1-800-525-6285

Experian: P.O. Box 2104, Allen, TX 75013, www.experian.com, 1-888-397-3742

TransUnion: P.O. Box 2000, Chester, PA 19022, www.transunion.com, 1-800-680-7289

Annual Credit Report. You may also order a free annual credit report. To do so, please visit www.annualcreditreport.com or call 1-887-322-8228.

You can also order your free annual credit report by mailing a completed Annual Credit Report Request Form (available from the U.S. Federal Trade Commission's ("FTC") website at www.consumer.ftc.gov/articles/0155-free-credit-reports) to: Annual Credit Report Request Service, P.O. Box 105281, Atlanta, GA 30348-5281.

> **For Colorado, Georgia, Maine, Maryland, Massachusetts, New Jersey, Puerto Rico, and Vermont residents**: You may obtain one or more (depending on the state) additional copies of your credit report, free of charge. You must contact each of the credit reporting agencies directly to obtain such additional report(s).

Fraud Alert. You may place a fraud alert in your file by contacting one of the three nationwide credit reporting agencies listed above. A fraud alert tells creditors to follow certain procedures, including contacting you before they open any new accounts or change your existing accounts. For that reason, placing a fraud alert can protect you, but also may delay you when you seek to obtain credit.

Security Freeze. You have the ability to place a security freeze on your credit report. A security freeze will prevent new credit from being opened in your name without the use of a PIN number that will be issued to you when you initiate the freeze. A security freeze is designed to prevent potential creditors from accessing your credit report without your consent. As a result, using a security freeze may interfere with or delay your ability to obtain credit. You must separately place a security freeze on your credit file with each credit reporting agency. To place a security freeze, you may be required to provide the credit reporting agency certain identifying information, including your full name; Social Security number; date of birth; current and previous addresses; a copy of your state-issued identification card; and a recent utility bill, bank statement, or insurance statement.

> **For Massachusetts and Rhode Island residents**: The consumer reporting agencies may require you to pay a fee to place, lift, or remove the security freeze. For Massachusetts residents, such fee may be up to $5.

Federal Trade Commission and State Attorneys General Offices. If you believe you are the victim of identity theft or have reason to believe your personal information has been misused, you should immediately contact the Federal Trade Commission and/or the Attorney General's office in your home state. You can also contact these agencies for information on how to prevent or avoid identity theft.

> You may contact the **Federal Trade Commission**, Consumer Response Center, 600 Pennsylvania Avenue, NW, Washington, DC 20580, www.ftc.gov/ IDTHEFT, 1-877-IDTHEFT (438-4338).
>
> **For Maryland residents**: You may contact the Office of the Maryland Attorney General, 200 St. Paul Place, Baltimore, MD 21202, http://www.marylandattorneygeneral.gov/, 1-888-743-0023.
>
> **For North Carolina residents**: You may contact the North Carolina Office of the Attorney General, Mail Service Center 9001, Raleigh, NC 27699-9001, http://www.ncdoj.gov/, 1-877-566-7226.
>
> **For Rhode Island residents**: You may contact the Rhode Island Office of the Attorney General, 150 South Main Street, Providence, RI 02903, http://www.riag.ri.gov, 401-274-4400.

Reporting identity theft and obtaining a police report.

For Iowa residents: You are advised to report any suspected identity theft to law enforcement or to the Iowa Attorney General.

For Massachusetts residents: You have the right to obtain a police report regarding this incident. If you are the victim of identity theft, you also have the right to file a police report and obtain a copy of it.

For Oregon residents: You are advised to report any suspected identity theft to law enforcement, including the Federal Trade Commission and the Oregon Attorney General.

For Rhode Island residents: You have the right to file or obtain a police report regarding this incident.

Federal Fair Credit Reporting Act Rights: The Fair Credit Reporting Act (FCRA) is federal legislation that regulates how consumer reporting agencies use your information. It promotes the accuracy, fairness, and privacy of consumer information in the files of consumer reporting agencies. As a consumer, you have certain rights under the FCRA, which the FTC has summarized as follows: you must be told if information in your file has been used against you; you have the right to know what is in your file; you have the right to ask for a credit score; you have the right to dispute incomplete or inaccurate information; consumer reporting agencies must correct or delete inaccurate, incomplete, or unverifiable information; consumer reporting agencies may not report outdated negative information; access to your file is limited; you must give your consent for reports to be provided to employers; you may limit "prescreened" offers of credit and insurance you get based on information in your credit report; you may seek damages from violators. Identify theft victims and active duty military personnel have additional rights. For more information about these rights, you may go to www.ftc.gov/credit or write to: Consumer Response Center, Room 13-A, Federal Trade Commission, 600 Pennsylvania Ave. N.W., Washington, D.C. 20580.