

# CLARK HILL

---

Robert A. Stern  
T 312.985.5940  
F 312.985.5955  
Email: rastern@clarkhill.com

Clark Hill  
130 East Randolph Street  
Suite 3900  
Chicago, IL 60601  
T 312.985.5900  
F 312.985.5999

[clarkhill.com](http://clarkhill.com)

May 18, 2021

**Attorney General Aaron Frey**  
Office of the Attorney General  
6 State House Station  
Augusta, ME 04333

Dear Attorney General Aaron Frey:

We represent Florida League of Cities, Inc. (“FLC”) with respect to a data security incident involving FLC’s third party service provider, Netgain Technology, LLC (“Netgain”). FLC is committed to answering any questions you may have about the data security incident, its response, and steps it has taken to prevent a similar incident in the future.

## **1. Nature of security incident.**

Netgain recently informed FLC that an unauthorized third party gained access to servers within the Netgain environment on December 3, 2020, including a server that hosted FLC’s data. Upon receiving notice from Netgain, FLC worked with Netgain and law enforcement to investigate this incident. After consulting with forensic investigators and law enforcement, FLC learned that this type of cyberattack is typically conducted for financial gain from the data hosting provider and attackers are not usually interested in retaining personal information. Additionally, Netgain apparently received assurances from the attacker that no data was retained and has confirmed with law enforcement that no FLC data has been posted online.

FLC investigated the data potentially impacted by this incident but due to limitations imposed by the volume and structure of the data at issue, was unable to specifically determine with a high degree of certainty what data may have been involved. Our review of FLC systems and databases concluded on April 20, 2021. It appears that employee and contractor information, individual participants in the Florida Municipal Pension Trust Fund (“FMPTF”), and individuals that paid to register for an event held by the Florida City and County Managers Association, Inc. (“FCCMA”) may have had information impacted as a result of this event. This information could have included individuals’ names, Social Security numbers, and/or date of birth. For those with information provided to FLC for FCCMA, credit card number and 3-digit CVV code information may have been impacted. While Netgain and FLC believe any risk of harm to employees and customers is low, FLC notified individuals whose contact information was present on FLC databases, posted a website notice, and notified prominent media of the event.

May 18, 2021

Page 2

**2. Number of Maine residents affected.**

FLC sent written notice to one (1) resident whose information may have been processed by FLC. The notification letter was sent to the potentially affected individuals on May 18, 2021 via regular mail (a copy of one of the template notification letters is enclosed).

**3. Steps taken or plan to take relating to the incident.**

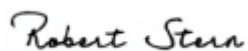
Upon learning of this incident, FLC terminated its relationship with Netgain and launched an investigation. To minimize the risk of future incidents, FLC is in the process of reviewing and updating its existing policies related to vendor data security and retention practices. FLC is offering employees and customers complimentary credit monitoring and identity restoration services for twelve months. FLC's mailed notice letter included information about the incident and instructions for enrolling in these services. Additionally, FLC posted notice on its website and notified prominent media outlets so that any individual participant in the FMPTF, a family member of a participant in the FMPTF, or anyone that paid to register for an event held by the FCCMA can enroll in 12 complimentary months of credit monitoring and identity restoration services by calling the number provided in any of those notices.

**4. Contact information.**

FLC takes the security of personal information in its or its third-party service providers' control seriously and is committed to protecting the personal information of its community. If you have any questions or need additional information, please do not hesitate to contact me at [Rastern@clarkhill.com](mailto:Rastern@clarkhill.com) or (312) 985-5940.

Very truly yours,

CLARK HILL



Robert A. Stern

cc: Jason Schwent

Enclosure

CLARK HILL



C/O IDX
10300 SW Greenburg Rd. Suite 570
Portland, OR 97223

To Enroll, Please Call:
1-833-903-3648
Or Visit:
https://app.idx.us/account-creation/protect
Enrollment Code: <<XXXXXXXXXX>>

<<First Name>> <<Last Name>>
<<Address1>> <<Address2>>
<<City>>, <<State>> <<Zip>>

May 18, 2021

Notice of Data Security Incident

Dear <<First Name>> <<Last Name>>,

Florida League of Cities, Inc. ("FLC") is writing to inform you of a data security incident involving its third-party data hosting provider, Netgain Technology, LLC ("Netgain") described in more detail below. FLC provides administrative and operational support services to various affiliate associations, including issuing payments to certain sole proprietors and similar individuals for services rendered to one or more of these affiliate associations. In the course of FLC's administrative services for these affiliate associations, your information may have been included in our systems among data stored with Netgain. FLC takes the privacy and security of your information seriously and sincerely apologizes for any concern or inconvenience this may cause you. This letter contains information about steps you can take to protect your information, and resources we are making available to help you.

1. What happened?

Netgain recently informed FLC that an unauthorized third party gained access to servers within the Netgain environment on December 3, 2020, including a server that hosted FLC's data. Upon receiving notice from Netgain, FLC worked with Netgain and law enforcement to investigate this incident. After consulting with forensic investigators and law enforcement, we learned that this type of cyberattack is typically for financial gain from the data hosting provider and attackers are not usually interested in retaining personal information. Additionally, Netgain received assurances from the attacker that no data was retained, and we have confirmed with law enforcement that no FLC data has been posted online. FLC investigated the data potentially impacted by this incident but due to some of the limitations imposed by the volume and structure of the data at issue, we were unable to specifically determine what data may have been involved. Therefore, out of an abundance of caution, we are providing notice of this incident for the benefit of all individuals whose personal information has been processed as part of our services.

2. What information was involved?

Our review of the impacted systems and databases to determine what information may be at risk concluded on April 20, 2021. It appears information provided to FLC in IRS 1099 forms, which was required to issue payments to sole proprietors and similar individuals for services rendered to one or more affiliate associations, was stored on the impacted systems and may have been affected. The 1099 form information included name, address, Social Security Number or Tax Identification Number. Although we have no evidence that your information was accessed, misused or even viewed, we wanted to let you know about this incident out of an abundance of caution.

### **3. What are we doing?**

In response to this incident, we notified law enforcement, consulted with Netgain, and hired an independent third-party data forensics expert to assist in analyzing the incident and data that may be at risk. We have since terminated our relationship with Netgain and we are in the process of reviewing existing policies and practices relating to vendor data security. Netgain has also assured us they are monitoring the dark web for any data related to this event and no such data has been discovered. Finally, we are also offering you complimentary credit monitoring services for <<12/24>> months, which are described in more detail below.

### **4. What can you do?**

The confidentiality and security of your information is of the utmost importance to us. While we believe the risk of any identity theft from this incident is low based on the nature of the incident and consultation with federal law enforcement, we are offering identity theft protection services through IDX, the data breach and recovery services expert. IDX identity protection services include: <<12/24>> months of credit and CyberScan monitoring, a \$1,000,000 insurance reimbursement policy, and fully managed id theft recovery services. With this protection, IDX will help you resolve issues if your identity is compromised.

You can contact IDX with any questions and to enroll in free identity protection services by calling 1-833-903-3648 or going to <https://app.idx.us/account-creation/protect> and using the Enrollment Code provided at the top of this letter. IDX representatives are available Monday through Friday from 9 am – 9 pm Eastern Time. Please note the deadline to enroll is August 18, 2021.

We encourage you to take full advantage of this service offering. Additional information about protecting your identity is included in this letter, including recommendations by the Federal Trade Commission regarding identity theft protection and details on how to place a fraud alert or a security freeze on your credit file. We also encourage you to review your account statements and explanation of benefits, and to monitor your credit report for suspicious activity.

### **5. For more information**

If you have any questions or concerns, please call 1-833-903-3648 Monday through Friday from 9 am – 9 pm Eastern Time or go to <https://app.idx.us/account-creation/protect>. Your trust is our top priority, and we deeply regret any inconvenience or concern that this matter may cause you.

Sincerely,

Florida League of Cities



## Recommended Steps to Help Protect Your Information

**1. Website and Enrollment.** Go to <https://app.idx.us/account-creation/protect> and follow the instructions for enrollment using your Enrollment Code provided at the top of the letter.

**2. Activate the credit monitoring** provided as part of your IDX identity protection membership. The monitoring included in the membership must be activated to be effective. Note: You must have established credit and access to a computer and the internet to use this service. If you need assistance, IDX will be able to assist you.

**3. Telephone.** Contact IDX at 1-833-903-3648 to gain additional information about this event and speak with knowledgeable representatives about the appropriate steps to take to protect your credit identity.

**4. Review your credit reports.** We recommend that you remain vigilant by reviewing account statements and monitoring credit reports. Under federal law, you also are entitled every 12 months to one free copy of your credit report from each of the three major credit reporting companies. To obtain a free annual credit report, go to [www.annualcreditreport.com](http://www.annualcreditreport.com) or call 1-877-322-8228. You may wish to stagger your requests so that you receive a free report by one of the three credit bureaus every four months.

If you discover any suspicious items and have enrolled in IDX identity protection, notify them immediately by calling or by logging into the IDX website and filing a request for help.

If you file a request for help or report suspicious activity, you will be contacted by a member of our ID Care team who will help you determine the cause of the suspicious items. In the unlikely event that you fall victim to identity theft as a consequence of this incident, you will be assigned an ID Care Specialist who will work on your behalf to identify, stop and reverse the damage quickly.

You should also know that you have the right to file a police report if you ever experience identity fraud. Please note that in order to file a crime report or incident report with law enforcement for identity theft, you will likely need to provide some kind of proof that you have been a victim. A police report is often required to dispute fraudulent items. You can report suspected incidents of identity theft to local law enforcement or to the Attorney General.

**5. Place Fraud Alerts** with the three credit bureaus. If you choose to place a fraud alert, we recommend you do this after activating your credit monitoring. You can place a fraud alert at one of the three major credit bureaus by phone and also via Experian's or Equifax's website. 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. The contact information for all three bureaus is as follows:

### Credit Bureaus

Equifax Fraud Reporting  
1-866-349-5191  
P.O. Box 105069  
Atlanta, GA 30348-5069  
[www.equifax.com](http://www.equifax.com)

Experian Fraud Reporting  
1-888-397-3742  
P.O. Box 9554  
Allen, TX 75013  
[www.experian.com](http://www.experian.com)

TransUnion Fraud Reporting  
1-800-680-7289  
P.O. Box 2000  
Chester, PA 19022-2000  
[www.transunion.com](http://www.transunion.com)

It is necessary to contact only ONE of these bureaus and use only ONE of these methods. As soon as one of the three bureaus confirms your fraud alert, the others are notified to place alerts on their records as well. You will receive confirmation letters in the mail and will then be able to order all three credit reports, free of charge, for your review. An initial fraud alert will last for one year.

**Please Note: No one is allowed to place a fraud alert on your credit report except you.**

**6. Security Freeze.** By placing a security freeze, someone who fraudulently acquires your personal identifying information will not be able to use that information to open new accounts or borrow money in your name. You will need to contact the three national credit reporting bureaus listed above to place the freeze. Keep in mind that when you place the freeze, you will not be able to borrow money, obtain instant credit, or get a new credit card until you temporarily lift or permanently remove the freeze. There is no cost to freeze or unfreeze your credit files.

**7. You can obtain additional information** about the steps you can take to avoid identity theft from the following agencies. The Federal Trade Commission also encourages those who discover that their information has been misused to file a complaint with them.

**California Residents:** Visit the California Office of Privacy Protection ([www.oag.ca.gov/privacy](http://www.oag.ca.gov/privacy)) for additional information on protection against identity theft.

**Kentucky Residents:** Office of the Attorney General of Kentucky, 700 Capitol Avenue, Suite 118 Frankfort, Kentucky 40601, [www.ag.ky.gov](http://www.ag.ky.gov), Telephone: 1-502-696-5300.

**Maryland Residents:** Office of the Attorney General of Maryland, Consumer Protection Division 200 St. Paul Place Baltimore, MD 21202, [www.oag.state.md.us/Consumer](http://www.oag.state.md.us/Consumer), Telephone: 1-888-743-0023.

**New Mexico Residents:** You have rights pursuant to the Fair Credit Reporting Act, such as the right to be told if information in your credit file has been used against you, the right to know what is in your credit file, the right to ask for your credit score, and the right to dispute incomplete or inaccurate information. Further, pursuant to the Fair Credit Reporting Act, the 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 credit reports to be provided to employers; you may limit “prescreened” offers of credit and insurance you get based on information in your credit report; and you may seek damages from a violator. You may have additional rights under the Fair Credit Reporting Act not summarized here. Identity theft victims and active duty military personnel have specific additional rights pursuant to the Fair Credit Reporting Act. You can review your rights pursuant to the Fair Credit Reporting Act by visiting [www.consumerfinance.gov/f/201504\\_cfpb\\_summary\\_your-rights-under-fcra.pdf](http://www.consumerfinance.gov/f/201504_cfpb_summary_your-rights-under-fcra.pdf), or by writing Consumer Response Center, Room 130-A, Federal Trade Commission, 600 Pennsylvania Ave. N.W., Washington, D.C. 20580.

**New York Residents:** the Attorney General may be contacted at: Office of the Attorney General, The Capitol, Albany, NY 12224-0341; 1-800-771-7755; <https://ag.ny.gov/>.

**North Carolina Residents:** Office of the Attorney General of North Carolina, 9001 Mail Service Center Raleigh, NC 27699-9001, [www.ncdoj.gov](http://www.ncdoj.gov), Telephone: 1-919-716-6400.

**Oregon Residents:** Oregon Department of Justice, 1162 Court Street NE, Salem, OR 97301-4096, [www.doj.state.or.us/](http://www.doj.state.or.us/), Telephone: 877-877-9392

**Rhode Island Residents:** Office of the Attorney General, 150 South Main Street, Providence, Rhode Island 02903, [www.riag.ri.gov](http://www.riag.ri.gov), Telephone: 401-274-4400

**All US Residents:** Identity Theft Clearinghouse, Federal Trade Commission, 600 Pennsylvania Avenue, NW Washington, DC 20580, [www.consumer.gov/idtheft](http://www.consumer.gov/idtheft), 1-877-IDTHEFT (438-4338), TTY: 1-866-653-4261.