# FREQUENTLY ASKED QUESTIONS
# DATA / PHISHING INCIDENT

## CONTACT INFORMATION

- Reporter/media, please call Joel Sappell, Countywide Public Information Officer at 213-974-1311 or contact him by email at jsappell@ceo.lacounty.gov

- Individuals who believe they may be affected may call 1-855-330-6368.

- The following departments sent notices to potentially affected individuals: Assessor, Chief Executive Office, Children and Family Services, Child Support Services, Health Services, Human Resources, Internal Services, Mental Health, Probation, Public Health, Public Library, Public Social Services, and Public Works.

### 1. WHAT HAPPENED?

On May 13, 2016, the County experienced a phishing email attack that affected approximately 108 County employee email accounts. A phishing email tries to trick someone in an attempt to acquire important information such as computer account usernames and passwords by sending an email that looks like it is coming from a trustworthy source.

### 2. WHAT INFORMATION WAS POTENTIALLY COMPROMISED?

Personal and/or health information of individuals who received County services or employees of the County were identified in some of these email accounts.

The information may have included first and last name, date of birth, Social Security Number (SSN), driver's license or state identification number, home address, phone number, payment card information, bank account information, and/or medical information, such as Medi-Cal or insurance carrier identification number, diagnoses, treatment histories, or medical record number.

### 3. WHY DID IT TAKE SO LONG FOR THE COUNTY TO NOTIFY INDIVIDUALS OF THE INCIDENT?

Due to an ongoing investigation, law enforcement instructed the County to delay providing notice to potentially affected individuals, because providing notice may have hindered law enforcement's criminal investigation.

We initiated notifications to the potentially affected individuals as soon as the law enforcement delay was lifted and we had confirmed individuals' identities and addresses.

## 4. HOW WILL I KNOW IF I AM AFFECTED?

Beginning on December 15, 2016, notices were mailed to potentially affected individuals at their last known address. However, if you recently moved or have not provided an address when you received care or services, you may not receive a letter. In addition, we have a call center (1-855-330-6368) where individuals may call to determine whether they have been affected by this incident.

## 5. WHAT IS THE COUNTY DOING IN RESPONSE TO THIS INCIDENT?

Law enforcement was notified upon discovery of the phishing attack and they are actively investigating this incident.

The County initiated an administrative review and implemented additional controls to minimize the risk of future phishing attacks against County email accounts, as well as enhanced specific employee training to identify and respond to phishing attacks as part of the County's ongoing cyber-security awareness campaign.

In addition to notifying individuals potentially impacted by this incident, we have notified the California Department of Public Health, the State Attorney General's Office, the U.S. Department of Health & Human Services' Office for Civil Rights, and other agencies as required by law and/or contract. We are seeking to stay ahead of the rapidly evolving and continuous threats to our systems. The County remains vigilant in its efforts to protect confidential information and continues to strengthen the information privacy and security program to implement safeguards to prevent and/or reduce cyber-attacks.

## 6. WHAT PROTECTION IS THE COUNTY OFFERING INDIVIDUALS AFFECTED BY THIS INCIDENT?

We are offering affected individuals' identity monitoring for one year at no cost, as well as other helpful information on how to protect against identity fraud and theft. Identity monitoring services include credit monitoring, identity consultation, and identity restoration.

## 7. WHO IS RESPONSIBLE FOR THE EMAIL PHISHING ATTACK?

The County is actively cooperating with the District Attorney's Cyber Investigative Response Team on the criminal investigation to determine who is responsible for the phishing attack and to file criminal charges against those responsible. An arrest warrant

issued for Austin Kelvin Onaghinor of Nigeria. He was charged with nine counts, including unauthorized computer access and identity theft.

## 8. ARE THERE STEPS I CAN TAKE TO PROTECT MYSELF FROM IDENTITY THEFT OR FRAUD?

We encourage you to remain vigilant against incidents of identity theft and fraud, to review your account statements, and to monitor your credit reports and explanation of benefits forms for suspicious activity. Under U.S. law, you are entitled to one free credit report annually from each of the three major credit reporting bureaus. To order your free credit report, visit www.annualcreditreport.com or call, toll-free, 1-877-322-8228. You may also contact the three major credit bureaus directly to request a free copy of your credit report or to place a fraud alert or security freeze on your credit file:

| Equifax | Experian | TransUnion |
|---|---|---|
| **P.O. Box 105069** | **P.O. Box 2002** | **P.O. Box 2000** |
| **Atlanta, GA 30348** | **Allen, TX 75013** | **Chester, PA 19022-2000** |
| **800-525-6285** | **888-397-3742** | **800-680-7289** |
| **www.equifax.com** | **www.experian.com** | **www.transunion.com** |

## 9. QUESTIONS REGARDING MINORS

Minors, under the age of eighteen (18), determined to have been potentially affected, may be enrolled in identity consultation and identity restoration services. Our call center can provide information to address concerns regarding a minor potentially affected by this incident to parents or legal guardians. For minors potentially affected through a DCFS email account, that same information may be provided to the minor's dependency attorney, DCFS social worker or caretaker.