170893

18TH JUDICIAL DISTRICT
PARISH OF POINTE COUPEE
STATE OF LOUISIANA

ITEM NUMBER: 17-2032 **WARRANT NUMBER:** LSP_2017_001494

AFFIDAVIT FOR ARREST WARRANT

STATE OF LOUISIANA
VERSUS
PRAKASH B RAYAMAJHI, White Male
9 Dyer Ct Apt B-1 , Danvers, MA, 01923
[redacted]
Height: 5'10", Weight: 175
Color: Brown, Hair Color: Black
D/M:

I, Alexandr Nezgodinsky , with the Louisiana State Police, certify under oath based on the information outlined below, that there is probable cause to believe PRAKASH B RAYAMAJHI on or about 01/27/2017 did commit:

1 Count of RS14:73.7 D--Computer Tampering (Felony)-- (FELONY)
5 Counts of RS14:73.10--Online Impersonation-- (FELONY)
1 Count of RS14:73.5--Computer Fraud-- (FELONY)
1 Count of RS14:67.20--Theft of a Business Record-- (FELONY)
247 Counts of RS14:67.16 C(1-3)--Identity Theft (Felony)-- (FELONY)
12 Counts of RS14:71.1--Bank Fraud-- (FELONY)
12 Counts of RS14:72--Forgery-- (FELONY)
12 Counts of RS14:230--Money Laundering; Transactions Involving Proceeds of Criminal Activity-- (FELONY)
1 Count of RS15:1353--Prohibited Activities; Racketeering-- (FELONY)

within this State and Parish at: and the jurisdiction of the 18TH Judicial District Court, contrary to the form of the statutes of the State of Louisiana in such case made and provided, and against the peace and dignity of the same, in that the following did occur:

On February 14, 2017, Courtney Gremillion, notified our Insurance Fraud / Auto Theft Unit that her identity had been stolen. She said that her accountant informed her that the IRS rejected her tax return because someone had already filed using her social security number. She stated she believes it was a result of email "phishing email scam" that took place at her place of employment a couple weeks prior.

Tuesday, July 18, 2017 19:29:10

Gremillion stated that she is employed as a Register Nurse for the Pointe Coupee General Hospital. The hospital is located at 2202 False River Drive, New Roads, La 70760. She stated she was informed by her supervisor at the hospital that someone, somehow, got a hold of all the employee's W2 forms. She said immediately following the incident, the hospital gave each employee printouts of "How to Battle ID Theft". She said this identity theft incident happened on January 27, 2017. Gremillion stated around February 6th, her accountant, John Hogan, 105 Gisele Street, New Roads, La. informed her that her tax submittal was rejected.

On February 16, 2017, Sgt. Eric Adams and I went to the Pointe Coupee Sheriff's Office to follow up on any existing investigation they may have regarding the breach. The detectives stated they were aware of the situation because the hospital administration had called and informed them. Detective Ferrall Foster stated they do not have an active investigation, but they do take the complaints from each employee and then assign them a report number. He said it is his understanding that the report number is needed for IRS purposes. He said they received half a dozen complaints from hospital employees so far.

On February 16, 2017, after leaving the S.O., Sgt. Adams and I went to Gremillion's Certified Public Accountant's office. CPA John Hogan (New Roads, La) informed us that he has done Courtney Gremillion's taxes for years and has never had a problem until now. He said he filed Courtney and her husband's taxes on February 8, 2017, and received a "rejection number IND510" on February 10, 2017. Hogan stated the rejection was due to Courtney Gremillion's social security number had already been filed in association with an earlier tax return. Hogan stated the next step was for Gremillion to fill out form 14-039 Victim of ID Theft.

On February, 23, 2017, Sgt. Eric Adams and I met with CFO John Cazayoux and CEO Chad Olinde regarding the breach. Also in attendance was hospital Attorney Jody Thibaut, Human Resource Director Lisa Patterson and Hospital Technical Support Engineer Anthony Sauro. The meeting was held at the hospital. Synopsis of the meeting is as follows:

On Friday, January 27, 2017, at 8:05am, CFO John Cazayoux, purportedly received an email from CEO Chad Olinde. John is the CFO of Pointe Coupee General Hospital in New Roads, Louisiana. Chad is the CEO of the same hospital. Their offices are both located in the hospital near each other. Their offices are separated by the secretary's office. John received five emails total that Friday, and he only replied to one.

John said the email appeared to be from "Chad Olinde", but upon further inspection, the email is **raymai6rvx6r@comcast.net**, which is not affiliated with Chad or the hospital.

The subject of the email was: EMPLOYEES 2016.

The body of the email read:

John,

I want you to send me the list of W-2 copy of employees wage and tax statement for 2016, I need them in PDF file type, you can send it as an attachment. Kindly prepare the lists and email them to me asap. Thanks. Chad Olinde

Sent from my iphone

Tuesday, July 18, 2017 19:29:10

Approximately one hour after receiving this email, John attached 235 hospital employee W-2's and sent them to the Comcast email. The W-2's consisted of employee name, employee home address and employee social security number. John sent the employee W-2 files in a PDF file. John stated it didn't take much time to run a report in the hospital computer system in order to gather the requested personnel files.

Later than morning John asked Chad if he received the files and Chad replied, "what files?" This is when they discovered that Chad did not send the email.

8:05am. - First email was sent to John requesting list of W-2's.

9:18am. - John replied and sent the W-2's.

Three additional email requests from "Chad Olinde" to John followed. All three emails had the same message:

John, I received the PDF File but I still need names, addresses, phone numbers and date of birth of all employees. I want it in Excel File. Thanks. Chad Olinde.. Sent from my iphone.

The times John received the above three emails:

9:30am

9:45am

9:55am

The fifth and final email John received from "Chad Olinde" was at 10:20am, and it read:

John, did you received my previous email? Write back. Thanks. Chad Olinde. Sent from my iphone.

Chad stated the first thing they did was to contact Anthony at their IT Department to see if they could take back the email that John sent, but they learned they could not do that. Chad also stated that they had gone to a "cyber conference" a week earlier so they called the instructors and then they called their insurance company. The insurance company informed them that the breach was more than likely directed at tax returns. Chad and John stated they also called the IRS, but they learned each employee must report the breach individually. They said they had a department manager meeting that day at 2:00pm to see what direction they wanted to go in. They said they wanted to go ahead and notify all employees, but they really didn't have much information to give them, so some employees went out and got Lifelock. In the meeting, John stated he was told to file his taxes as soon as possible. They said the insurance company recommended an attorney out of Oregon and they believe he called the FBI. They said their hospital insurance includes 'cyber coverage'. John stated that he knows of twelve (12) employees that have tried to file their taxes and their return was rejected because someone had used their social security number to file.

Sgt. Adams then asked if this breach could have been done by someone local or an ex-employee. Anthony, with the hospital IT Department answered, the format of the email matched identically from the FBI, almost word for word. Sgt. Adams asked who the the "cyber insurance" is with and Chad answered that the hospital is self-insured through HSLI which is a subsidery of Louisiana Hospital Association. Sgt. Adams asked if Courtney Gremillion would be covered under this "cyber insurance" and Chad stated, "that is a good question, probably just the hospital

itself." He continued to state they did "purchase ID Theft protection through ID Experts and that is supposed to provide a million dollars in coverage for each one of these employees and they each have their own individual account so if someone taps into Courtney's bank she would be covered through that insurance". Sgt. Adams asked if the hospital purchased the coverage for the employees after the breach, would they still be covered. They answered the coverage was purchased that Monday following the breach and they should be covered. They stated the coverage is called ID Experts and its good for three years for every employee, but the employee must sign up for it.

Anthony stated this was a traditional spear phishing attack where they identified the CEO and CFO. He said John said the English was good so it didn't throw up any red flag. Anythony said but the "reply to address" was a Comcast domain address. John stated "I just didn't catch that." Anthony stated once you hit reply is when you can see that it a Comcast address and not Chad's address. Anthony states that you can also see it's a Comcast address if you "hover over it".

Sgt. Adams asked if the hospital website identifies John and Chad and their positions? They answered yes.

Anthony stated that these phishing emails are common knowledge, but they weren't proactive.

The hospital immediately notified the employees of their mistake and CEO Chad Olinde issued a statement. The statement is as followed:

MEDIA STATEMENT FROM POINTE COUPEE GENERAL HOSPITAL

EMPLOYEES NOTIFIED OF DATA SECURITY INCIDENT

New Roads, Louisiana: Pointe Coupee General Hospital is in the process of formally notifying 235 employees of a data security incident that affected their W-2 information. The incident occurred on Friday, January 27, at which time employees were informally notified that their information was accessed without authorization. Pointe Coupee General Hospital has since engaged ID Experts to provide (24 or 36) months of credit monitoring and identity remediation services to the affected employees. Pointe Coupee General Hospital also reported the matter to the Internal Revenue Service/Criminal Investigation in an attempt to prevent fraudulent activity and to hold the perpetrators accountable. Chief Executive Officer Chad Olinde stated that "We take the privacy and security of our employee information very seriously. We are working with ID Experts to provide our

employees the resources to protect their information, and will provide whatever cooperation is necessary for the IRS/CI to hold the perpetrators accountable."

On March 27, 2017, I got a search warrant signed by Judge James Best of the 18th JDC. The warrant was to search the **raymal6rvx6r@comcast.net** account.

On April 3, 2017, I faxed the search warrant to the Comcast Legal Team regarding the email address.

I informed them that the information contained in the email server was essential in proving the location of the computer used to send this phishing email scam. The Legal Department at Comcast had been contacted and their custodian of records was awaiting the issuance of a Search Warrant to release the documents of this account. They asked that the Search Warrant for the

things specified in this affidavit be issued via facsimile machine and that they intend to honor the decisions of the Court and the Laws of the State of Louisiana.

On April 25, 2017, I received an envelope in the mail from Comcast Legal Response Center, Moorestown, NJ. In the envelope were a three-page face sheet and a CD disc. On the face sheet Comcast stated the subscriber information for raymai6rvx6r@comcast.net, is as follows:

Subscriber Name:	Parkash Rayamajhi
Service Address:	9B Dyer Ct. Apt. 1, Danvers, MA 019232646
Billing Address:	9 Dyer Ct. Apt. B1, Danvers, MA 01923
Telephone#:	978-750-1011
Type of Service:	High Speed Internet
Account Number:	8773103940335649
Account Status:	Active
IP Assignment:	Dynamically Assigned
Email User IDs:	RAYAMAJHI6rvx6r, raymaI6rvx6r

Comcast also indicated that the account indicates a start date of December 27, 2016 and an end date of March 27, 2017.

On the disc was a file titled "final web auth logs". Within the logs were 131 authenification log events. Brousing the 131 log events indicates that raymaI6rvx6r@comcast.net continuously sent out phishing emails to various corporations and businesses throughout the United States. One of the logs indicated a path to jcazayoux@pcgh.org dated Friday, January 27, 2017. The log also verifies the statements from PCGH regarding the circumstances surrounding the breach. The log has captured all emails sent and received by both parties.

On Tuesday, May 23, 2017, Sgt. Adams requested the State Police Intelligence Unit to conduct a workup on the findings of the search warrant. The results indicated and verified the information supplied by Comcast Legal Center. The address and phone number come back to:

Name:	Parkash B. Rayamajhi
DOB:	06/17/1968
SSN:	011-90-3247
TX DL:	29508137
MA DL:	S25820551

As a result of this investigation, it has been determined that Parkash Rayamajhi is responsible or a conspirator to orchestrating a phishing email scheme targeting the CEO and CFO of Pointe Coupee General Hospital in New Roads, Louisiana.

Tuesday, July 18, 2017 19:29:10

Five emails (Computer Tampering) were sent to PCGH purporting to be from CEO Chad Olinde. (Online Impersonation) As a result of these emails, an email (Computer Fraud & Theft of a Business Record) was sent from PCGH and that email contained the identity of 235 W-2 records of Pointe Coupee Hospital Employees. These records contained the employee's name, address and social security number. (Identity Theft). Twelve of these social security numbers were used to file tax returns with the United States Internal Revenue Service (Bank Fraud, Forgery & Identity Theft).

Parkash Rayamajhi actions result in a violation of:

LRS 14:73.7	Computer Tampering (1 Count)
LRS 14:73.10.	Online Impersonation (5 Counts)
LRS 14:73.5.	Computer Fraud (1 Count)
LRS 14:67:20.	Theft of a Business Record (1 Count)
LRS 14:67.16	Identity Theft (247 Counts) (235 Employee W2 & 12 Counts for IRS returns)
LRS 14:71:1.	Bank Fraud (Financial Institution) (12 Counts)
LRS 14:72.	Forgery (12 Counts)
LRS 14:230.	Money Laundering (12 Counts)
LRS 15:1353	Racketeering (1 Count)

I hereby certify under oath the information contained herein to be true and correct, to the best of my knowledge, under penalties of perjury, so help me God.

Alexandr Nezgodinsky
Affiant

Tuesday, July 18, 2017 19:29:10