Notice of Data Security Incident

What Happened?

On April 1st, 2021, the Office of the Public Defender for the Twentieth Judicial Circuit of Florida was the victim of a malware attack. Upon discovery, the agency immediately cut access to all technological resources, contacted law enforcement, and assembled a team of experienced professionals to contain, investigate, and respond to the incident. Since that time, the agency's focus has been on creating new IT infrastructure to restore full functionality, and working with our data recovery team to safely regain access to the affected equipment.

The agency takes its role of safeguarding the personal information it is entrusted with very seriously. We are fully committed to protecting all confidential information and are keenly aware of how important this information is to everyone. While there is no evidence that confidential data has been accessed or misused, the agency is alerting individuals that may have been affected through public notification as a precautionary measure. We encourage all individuals to respond to this attack proactively.

What Information Was Involved?

The agency's computer system contains confidential personal information of employees and clients, both current and former. It is estimated that the agency maintains in excess of 500,000 personnel and client files. Information that may have been in the agency's files includes:

Client Information	Staff Information
• Names • Social security numbers • Copies of government-issued document numbers used to establish identity (e.g. driver's license, identification card) • Medical or mental health history information (in limited circumstances)	• Names • Social security numbers • Copies of government-issued documents and document numbers used to establish identity (e.g. driver's license, identification card) • Medical history information (e.g. FMLA/disability forms, if employee completed)

What You Can Do

While there is no evidence personal information has been accessed or will be used inappropriately, we encourage all individuals who could possibly be affected by this incident to remain vigilant against incidents of identity theft.

Steps all individuals can take to protect themselves now include:

Place a fraud alert on your credit. Anyone concerned about identity theft can place a fraud alert, which allows you to add a layer of protection to your credit file. A fraud alert ensures that companies verify your identity before providing new credit in your name. To place a fraud alert, you can contact any one of the three nationwide credit bureaus (Equifax, Experian, or TransUnion) and that one must notify the other two.

Information for the three nationwide credit bureaus is as follows:

Equifax	**Experian**	**TransUnion**
Phone: 1-800-685-1111 www.equifax.com	Phone: 1-888-397-3742 www.experian.com	Phone: 1-888-909-8872 www.transunion.com

Freeze your credit. Credit freezes restrict access to your credit file, making it harder for identity thieves to open new accounts in your name. You can freeze and unfreeze your credit for free. To freeze your credit, you will need to contact the three main credit bureaus: Equifax, Experian and TransUnion. You can locate the credit freeze information for all three credit bureaus by clicking these links: Equifax, Experian, TransUnion. These pages allow you to freeze your credit or unfreeze your credit and provide helpful information.

Check your credit report. Checking your credit reports periodically can help you spot problems and address them quickly. During the pandemic, everyone in the U.S. can get a free credit report each week from all three credit bureaus: Equifax, Experian, and TransUnion. To utilize this service, visit annualcreditreport.com.

Monitor your credit. Credit monitoring services allow you to safeguard your credit. These services notify you of changes made to your credit reports so you can take action against potential misuse of your personal information. Sign up for a credit monitoring service to allow you to stay on top of any changes to your credit. There are free credit monitoring services, including:

CreditWise from Capital One: https://creditwise.capitalone.com/

Experian: https://www.experian.com/consumer-products/credit-monitoring.html

Carefully review the statements sent from your insurance companies and medical providers. Health insurance companies routinely send out "explanation of benefits" summaries, detailing medical services rendered. These summaries are not bills, but rather explain what the insurance company has paid for. Review these summaries to make sure everything looks accurate. You should review everything mailed to you from all medical and insurance providers. If you notice anything looks suspicious, contact your provider or insurance company right away.

Visit the Federal Trade Commission's website for more information regarding identify theft and protecting your identity. See this link to learn more:

https://www.consumer.ftc.gov/topics/identity-theft

For More Information

If you have any questions regarding this incident, you may contact the Office of the Public Defender, 20th Judicial Circuit, by emailing support@PD20.org. You may also write to the agency at:

Office of the Public Defender, 20th Judicial Circuit
ATTN: Katie Downey, Director of Administration
PO Drawer 1980
Fort Myers, Florida 33902