



DESTIN REALTY

BEACH VACATION RENTALS & SALES

June 17, 2022

VIA ELECTRONIC MAIL

Office of the Maryland Attorney General
200 St. Paul Place
Baltimore, MD 21202

Delivered via email to: idtheft@oag.state.md.us

RE: Destin Realty, Inc. Security Incident

Dear Sir/Madam:

I am writing to notify you that Destin Realty, Inc.—a real estate company in Destin, Florida—determined on April 14, 2022, that a security incident it suffered resulted in the potential unauthorized access to individuals' personal information.

A third-party used a phishing attack to gain unauthorized access to some of Destin Realty, Inc.'s email accounts. The third-party had access between October 12, 2021, and January 19, 2022. On January 19th we retained outside counsel experienced in these matters and started working closely with a leading forensic/cybersecurity company to investigate the incident. As part of that investigation, we took measures to eliminate the third-party's access and secure our systems against future attacks. This included changing passwords and implementing multifactor authentication. Subsequently, the investigation identified which email accounts had been accessed, and we engaged a data review firm to identify whether those files contained personal information. The data review firm provided their report in April, and we have been working since then to assess our notification obligations and identify proper contact information for the affected individuals.

Having reviewed the data, we have reason to believe that the third-party potentially viewed the personal information of five Maryland residents. The unauthorized third-party gained access to some combination of individuals' names, contact information, medical information, government identification (such as a passport number, Social Security number, or driver's license number), financial account information (such as bank account and routing number), and login information for a limited subset of applications or websites. At this time, however, we have no reason to suspect the information was or will be misused. Consistent with our obligations under state law, we are notifying the affected individuals that their information may have been improperly accessed.

We have attached a template of the notices we are providing to Maryland residents. We are providing credit monitoring to people whose driver's license or Social Security numbers was affected. Please contact me if you have any questions or need any additional information regarding this incident.

Sincerely,

Jeffrey Sanders

Vice-President & Chief Operating Officer

Destin Realty
Mail Handling Services
777 E Park Dr
Harrisburg, PA 17111



C-1

[name]

[address]

[city], [state] [zip]

[date]

NOTICE OF DATA BREACH

Dear [name]:

We are writing to inform you about an incident that may have exposed your personal information to unauthorized persons.

WHAT HAPPENED

We determined that an unauthorized third-party gained access to a limited portion of Destin Realty, Inc.'s email system between October 12, 2021, and January 19, 2022. After discovering the incident in mid-January, we started working with third-party experts to investigate the incident and shortly thereafter engaged a data review to identify whose information may have been in the affected files.

WHAT INFORMATION WAS INVOLVED

In late April, we received the results from the data review firm. Based on those results, we determined that the unauthorized third-party accessed some of your personal information, which may include your full name, contact information, medical information, passport number, financial account information (such as bank account and routing number), and login information.

WHAT WE ARE DOING

We hired third-party experts to address this situation, perform an investigation into the unauthorized activity, and further bolster the security of our systems to protect your information.

WHAT YOU CAN DO

Remain vigilant – We encourage you to remain vigilant for fraud or identity theft by reviewing your account statements and free credit reports. You can also find additional suggestions at www.IdentityTheft.gov/DataBreach.

- You should confirm that your credit card company has the correct address on file for you and that all charges on the account are legitimate. If you discover errors or suspicious activity, you should immediately contact the credit card company and inform them that you have received this letter.
- You should obtain and review a free copy of your credit report by visiting www.annualcreditreport.com or calling (877) 322-8228. If the report is incorrect, you should contact the appropriate consumer reporting agency—Equifax, Experian, or TransUnion.

Consider placing a fraud alert or security freeze on your credit file – Consumer reporting agencies have tools you can use to protect your credit, including fraud alerts and security freezes.

- A fraud alert is a cautionary flag you can place on your credit file to notify companies extending you credit that they should take special precautions to verify your identity. You can contact any of the three consumer reporting agencies to place fraud alerts with each agency. The alert lasts for one year, but you can renew it.
- A security freeze is a more dramatic step that will prevent others from accessing your credit report, which makes it harder for someone to open an account in your name. You must contact each consumer reporting agency separately to order a security freeze, and they may require you to provide them with your full name, Social Security number, date of birth, and current and previous addresses. You can obtain more information about security freezes by contacting the consumer reporting agencies or the Federal Trade Commission.

Report suspicious activity – If you believe you are the victim of identity theft, consider (1) notifying your Attorney General, local law enforcement, or the Federal Trade Commission; (2) filing a police report and requesting a copy of that report; and (3) visiting IdentityTheft.gov to report the issue and get recovery steps.

Contact relevant authorities – You may contact the below resources to (1) get more information on fraud alerts or security freezes and (2) learn more about protecting yourself from fraud or identity theft.

TransUnion
P.O. Box 2000
Chester, PA 19016
(888) 909-8872
www.transunion.com

Equifax
P.O. Box 740241
Atlanta, GA 30374
(800) 685-1111
www.equifax.com

Experian
P.O. Box 9701
Allen, TX 75013
(888) 397-3742
www.experian.com

**Maryland
Attorney General**
200 St. Paul Place, 25th Floor
Baltimore, MD 21202
(888) 743-0023
www.marylandattorneygeneral.gov

**New York
Attorney General**
The Capitol
Albany, NY 1224
(800) 771-7755
www.ag.ny.gov

**Federal Trade
Commission**
600 Pennsylvania Ave. NW
Washington, DC 20580
(202) 326-2222
www.ftc.gov

You can also find your Attorney General's contact information at: <https://www.usa.gov/state-attorney-general>.

Review the Fair Credit Reporting Act – You also have certain rights under the Fair Credit Reporting Act (FCRA), including the right to know what is in your file, to dispute incomplete or inaccurate information, and to have consumer reporting agencies correct or delete inaccurate, incomplete, or unverifiable information. For more information about the FCRA, and your rights pursuant to the FCRA, please visit: <https://www.consumer.ftc.gov/articles/pdf-0096-fair-credit-reporting-act.pdf>.

FOR MORE INFORMATION

Protecting the privacy of your personal information is important to us, and we regret any inconvenience this incident may cause you. Please know that we are doing everything that we can to assist and guide you through this process. Should you have any questions or concerns, you can contact us at 888-875-5565 from 8:00 AM to 5:00 PM Central Time, Monday through Friday and one of our representatives will be happy to assist you. Thank you for your understanding and patience.

Sincerely,



Jeffrey Sanders
Vice-President & Chief Operating Officer

Destin Realty
Mail Handling Services
777 E Park Dr
Harrisburg, PA 17111



A-1

[name]

[address]

[city], [state] [zip]

[date]

NOTICE OF DATA BREACH

Dear [name]:

We are writing to inform you about an incident that may have exposed your personal information to unauthorized persons.

WHAT HAPPENED

We determined that an unauthorized third-party gained access to a limited portion of Destin Realty, Inc.'s email system between October 12, 2021, and January 19, 2022. After discovering the incident in mid-January, we started working with third-party experts to investigate the incident and shortly thereafter engaged a data review to identify whose information may have been in the affected files.

WHAT INFORMATION WAS INVOLVED

In late April, we received the results from the data review firm. Based on those results, we determined that the unauthorized third-party accessed some of your personal information, which may include your full name, contact information, medical information, government identification (such as a passport number, Social Security number, or driver's license number), financial account information (such as bank account and routing number), and login information.

WHAT WE ARE DOING

We hired third-party experts to address this situation, perform an investigation into the unauthorized activity, and further bolster the security of our systems to protect your information.

WHAT YOU CAN DO

Activate your complimentary credit monitoring – To help protect you from fraud or identity theft, we are offering a complimentary one-year membership to Experian's IdentityWorks. This product helps detect possible misuse of your personal information. To register, please:

- Ensure that you **enroll by: 9/7/2022** (Your code will not work after this date.)
- **Visit** the Experian IdentityWorks website to enroll: www.experianidworks.com/3bcredit
- Provide your **activation code**: [code]

If you have questions or want an alternative to enrolling in Experian IdentityWorks online, please contact Experian at (877) 288-8057 by 9/7/2022 and provide them engagement number [number].

Remain vigilant – We encourage you to remain vigilant for fraud or identity theft by reviewing your account statements and free credit reports. You can also find additional suggestions at www.IdentityTheft.gov/DataBreach.

- You should confirm that your credit card company has the correct address on file for you and that all charges on the account are legitimate. If you discover errors or suspicious activity, you should immediately contact the credit card company and inform them that you have received this letter.
- You should obtain and review a free copy of your credit report by visiting www.annualcreditreport.com or calling (877) 322-8228. If the report is incorrect, you should contact the appropriate consumer reporting agency—Equifax, Experian, or TransUnion.

Consider placing a fraud alert or security freeze on your credit file – Consumer reporting agencies have tools you can use to protect your credit, including fraud alerts and security freezes.

- A fraud alert is a cautionary flag you can place on your credit file to notify companies extending you credit that they should take special precautions to verify your identity. You can contact any of the three consumer reporting agencies to place fraud alerts with each agency. The alert lasts for one year, but you can renew it.
- A security freeze is a more dramatic step that will prevent others from accessing your credit report, which makes it harder for someone to open an account in your name. You must contact each consumer reporting agency separately to order a security freeze, and they may require you to provide them with your full name, Social Security number, date of birth, and current and previous addresses. You can obtain more information about security freezes by contacting the consumer reporting agencies or the Federal Trade Commission.

Report suspicious activity – If you believe you are the victim of identity theft, consider (1) notifying your Attorney General, local law enforcement, or the Federal Trade Commission; (2) filing a police report and requesting a copy of that report; and (3) visiting IdentityTheft.gov to report the issue and get recovery steps.

Contact relevant authorities – You may contact the below resources to (1) get more information on fraud alerts or security freezes and (2) learn more about protecting yourself from fraud or identity theft.

TransUnion
P.O. Box 2000
Chester, PA 19016
(888) 909-8872
www.transunion.com

Equifax
P.O. Box 740241
Atlanta, GA 30374
(800) 685-1111
www.equifax.com

Experian
P.O. Box 9701
Allen, TX 75013
(888) 397-3742
www.experian.com

**Maryland
Attorney General**
200 St. Paul Place, 25th Floor Baltimore,
MD 21202
(888) 743-0023
www.marylandattorneygeneral.gov

**New York
Attorney General**
The Capitol
Albany, NY 1224
(800) 771-7755
www.ag.ny.gov

**Federal Trade
Commission**
600 Pennsylvania Ave. NW
Washington, DC 20580
(202) 326-2222
www.ftc.gov

You can also find your Attorney General's contact information at: <https://www.usa.gov/state-attorney-general>.

Review the Fair Credit Reporting Act – You also have certain rights under the Fair Credit Reporting Act (FCRA), including the right to know what is in your file, to dispute incomplete or inaccurate information, and to have consumer reporting agencies correct or delete inaccurate, incomplete, or unverifiable information. For more information about the FCRA, and your rights pursuant to the FCRA, please visit: <https://www.consumer.ftc.gov/articles/pdf-0096-fair-credit-reporting-act.pdf>.

FOR MORE INFORMATION

Protecting the privacy of your personal information is important to us, and we regret any inconvenience this incident may cause you. Please know that we are doing everything that we can to assist and guide you through this process. Should you have any questions or concerns, you can contact us at 888-875-5565 from 8:00 AM to 5:00 PM Central Time, Monday through Friday and one of our representatives will be happy to assist you. Thank you for your understanding and patience.

Sincerely,



Jeffrey Sanders Vice-
President & Chief Operating Officer