CIPRIANI & WERNER

A PROFESSIONAL CORPORATION

ATTORNEYS AT LAW

450 Sentry Parkway, Suite 200
Blue Bell, PA 19422

Phone: (610) 567-0700
Fax: (610) 567-0712

www.C-WLAW.com

A Mid-Atlantic Litigation Firm

Visit us online at
www.C-WLAW.com

HILARY HIGGINS
HHiggins@c-wlaw.com

September 25, 2023

Via E-Mail (consumer@ag.iowa.gov)
Consumer Protection Division
Security Breach Notifications
Office of the Attorney General of Iowa
1305 E. Walnut Street
Des Moines, IA 50319

To Whom It May Concern:

We serve as counsel for Francesca's Acquisition, LLC ("Francesca's") located at 8760 Clay Road, Houston, TX 77080 and provide this notification to your Office of a recent data security incident suffered by Francesca's. By providing this notice, Francesca's does not waive any rights or defenses under Iowa law, including the data breach notification statute.

On January 31, 2023, Francesca's discovered a potential network disruption. Upon notification, Francesca's immediately took steps to secure its systems and engaged a third-party team of forensic investigators to determine the full nature and scope of the incident. Following a thorough investigation, Francesca's confirmed that a limited amount of information may have been impacted in connection with this incident. Francesca's undertook a meticulous review of the potentially impacted information with the assistance of a third-party data review team in order to identify what information, if any, belonging to individuals may have been impacted by this event.

On August 8, 2023, Francesca's determined that information related to five hundred forty-five (545) residents of the Iowa was potentially impacted by this event. The types of information impacted included Social Security number and/or financial account information. As our investigation is ongoing, we will provide supplemental notification should we determine additional Iowa residents are potentially affected.

Francesca's provided written notice of this incident to the potentially impacted Iowa residents on September 25, 2023, pursuant to the Iowa state law. A copy of the notice letter is attached hereto as **Exhibit A**, which provides details of the incident, complimentary credit monitoring services for twelve (12) months, and steps impacted individuals can take to protect their data.

Please contact me should you have any questions.

Very truly yours,

Hilary Higgins, Esquire
CIPRIANI & WERNER, P.C.

Exhibit A

francesca's

<<Date>> (Format: Month Day, Year)

<<first_name>> <<middle_name>> <<last_name>> <<suffix>>
<<address_1>>
<<address_2>>
<<city>>, <<state_province>> <<postal_code>>
<<country>>

<<b2b_text_1(Re: Notice of Data Breach)>>

Dear <<first_name>> <<middle_name>> <<last_name>> <<suffix>>:

We are writing to notify you of a recent incident at Francesca's Acquisition, LLC ("Francesca's"). We take the privacy and security of all information very seriously, and while we have no evidence to suggest that any information was subject to actual or attempted fraudulent misuse as a result of this incident, we are taking steps to proactively notify potentially impacted individuals out of an abundance of caution.

What Happened? On August 8, 2023, Francesca's learned that some of your information may have been impacted by an event experienced earlier this year. On January 31, 2023, Francesca's discovered a potential network disruption. Immediately upon discovery, Francesca's engaged a third-party team of forensic investigators to determine the full nature and scope of the incident. On August 8, 2023, following a thorough investigation, Francesca's confirmed that a limited amount of information related to you may have been impacted in connection with this incident.

What Information Was Involved? The potentially impacted information may have included your first name or initial and last name, in combination with <<b2b_text_2(data elements)>>.

What Are We Doing? Upon learning of this incident, we immediately took steps to secure our systems and investigate the incident. We implemented additional technical safeguards to further enhance the security of information in our possession. We arranged for complimentary identity monitoring for 12 months through Kroll. Due to privacy laws, we cannot activate these services and you will need to take steps to activate. The process to activate is outlined in this letter. We have also provided additional information about steps you can take to help protect yourself against fraud and identity theft.

What You Can Do. We recommend that you remain vigilant against incidents of identity theft and fraud by regularly reviewing your credit reports/account statements for suspicious activity and to detect errors. If you discover any suspicious or unusual activity on your accounts, please promptly contact the financial institution or company. You can also activate the complimentary identity monitoring as described below, and you can review the enclosed "Steps You Can Take to Help Protect Your Information" for additional resources.

For More Information. Should you have additional questions or concerns regarding this matter, please do not hesitate to contact our dedicated call center at TFN, Monday through Friday during the hours of 8:00 a.m. and 5:30 p.m CT., excluding some major U.S. holidays. You can also write us at 8760 Clay Road, Houston TX 77080.

Sincerely,

Andrew Clarke
Chief Executive Officer

STEPS YOU CAN TAKE TO HELP PROTECT YOUR INFORMATION

Activate Identity Monitoring Services

Visit **https://enroll.krollmonitoring.com** to activate and take advantage of your identity monitoring services.

You have until <<b2b_text_6(activation deadline)>> to activate your identity monitoring services.

Membership Number: **<<Membership Number s_n>>**

For more information about Kroll and your Identity Monitoring services, you can visit info.krollmonitoring.com.

KROLL

TAKE ADVANTAGE OF YOUR IDENTITY MONITORING SERVICES

You have been provided with access to the following services from Kroll:

Single Bureau Credit Monitoring

You will receive alerts when there are changes to your credit data—for instance, when a new line of credit is applied for in your name. If you do not recognize the activity, you'll have the option to call a Kroll fraud specialist, who will be able to help you determine if it is an indicator of identity theft.

Fraud Consultation

You have unlimited access to consultation with a Kroll fraud specialist. Support includes showing you the most effective ways to help protect your identity, explaining your rights and protections under the law, assistance with fraud alerts, and interpreting how personal information is accessed and used, including investigating suspicious activity that could be tied to an identity theft event.

Identity Theft Restoration

If you become a victim of identity theft, an experienced Kroll licensed investigator will work on your behalf to resolve related issues. You will have access to a dedicated investigator who understands your issues and can do most of the work for you. Your investigator will be able to dig deep to uncover the scope of the identity theft, and then work to resolve it.

Kroll's activation website is only compatible with the current version or one version earlier of Chrome, Firefox, Safari and Edge.

To receive credit services, you must be over the age of 18 and have established credit in the U.S., have a Social Security number in your name, and have a U.S. residential address associated with your credit file.

Monitor Your Accounts

We encourage you to remain vigilant against incidents of identity theft and fraud by reviewing your credit reports/account statements and explanation of benefits forms for suspicious activity and to detect errors. Under U.S. law, you are entitled to one free credit report annually from each of the three major credit reporting bureaus, TransUnion, Experian, and Equifax. To order your free credit report, visit www.annualcreditreport.com or call 1-877-322-8228. Once you receive your credit report, review it for discrepancies and identify any accounts you did not open or inquiries from creditors that you did not authorize. If you have questions or notice incorrect information, contact the credit reporting bureau.

You have the right to place an initial or extended "fraud alert" on a credit file at no cost. An initial fraud alert is a one-year alert that is placed on a consumer's credit file. Upon seeing a fraud alert, a business is required to take steps to verify the consumer's identity before extending new credit. If you are a victim of identity theft, you are entitled to an extended fraud alert lasting seven years. Should you wish to place a fraud alert, please contact any of the three credit reporting bureaus listed below.

As an alternative to a fraud alert, you have the right to place a "credit freeze" on a credit report, which will prohibit a credit bureau from releasing information in the credit report without your express authorization. The credit freeze is designed to prevent credit, loans, and services from being approved in your name without your consent. However, you should be aware that using a credit freeze may delay, interfere with, or prohibit the timely approval of any subsequent request or application you make regarding a new loan, credit, mortgage, or any other account involving the extension of credit. Pursuant to federal law, you cannot be charged to place or lift a credit freeze on your credit report. To request a credit freeze, you will need to provide the following information to the credit reporting agency:

1. Full name (including middle initial as well as Jr., Sr., III, etc.);
2. Social Security number;
3. Date of birth;

4. Address for the prior two to five years;
5. Proof of current address, such as a current utility or telephone bill;
6. A legible photocopy of a government-issued identification card (e.g., state driver's license or identification card); and
7. A copy of either the police report, investigative report, or complaint to a law enforcement agency concerning identity theft, if you are a victim of identity theft.

Should you wish to place a fraud alert or credit freeze, please contact the three major credit reporting bureaus listed below:

TransUnion 1-800-680-7289 www.transunion.com **TransUnion Fraud Alert** P.O. Box 2000 Chester, PA 19016-2000 **TransUnion Credit Freeze** P.O. Box 160 Woodlyn, PA 19094	**Experian** 1-888-397-3742 www.experian.com **Experian Fraud Alert** P.O. Box 9554 Allen, TX 75013 **Experian Credit Freeze** P.O. Box 9554 Allen, TX 75013	**Equifax** 1-888-298-0045 www.equifax.com **Equifax Fraud Alert** P.O. Box 105069 Atlanta, GA 30348-5069 **Equifax Credit Freeze** P.O. Box 105788 Atlanta, GA 30348-5788

Additional Information

You can further educate yourself regarding identity theft, fraud alerts, credit freezes, and the steps you can take to help protect your personal information by contacting the credit reporting bureaus, the Federal Trade Commission (FTC), or your state Attorney General. The FTC also encourages those who discover that their information has been misused to file a complaint with them. The FTC may be reached at 600 Pennsylvania Ave. NW, Washington, D.C. 20580; www.identitytheft.gov; 1-877-ID-THEFT (1-877-438-4338); and TTY: 1-866-653-4261.

You have the right to file a police report if you ever experience identity theft or fraud. Please note that in order to file a report with law enforcement for identity theft, you will likely need to provide some proof that you have been a victim. Instances of known or suspected identity theft should also be reported to law enforcement, your state Attorney General, and the FTC. This notice has not been delayed by law enforcement.

For District of Columbia residents, the District of Columbia Attorney General may be contacted at: 400 6th St. NW Washington, D.C. 20001; 202-442-9828, and https://oag.dc.gov/consumer-protection.

For Maryland residents, the Maryland Attorney General may be contacted at: 200 St. Paul Place, 16th Floor, Baltimore, MD 21202; 1-410-528-8662 or 1-888-743-0023; and https://www.marylandattorneygeneral.gov/.

For 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 bureaus 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 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. We encourage you to review your rights pursuant to the Fair Credit Reporting Act by visiting 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.

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

For North Carolina residents, the North Carolina Attorney General may be contacted at: 9001 Mail Service Center, Raleigh, NC 27699-9001; 1-877-566-7226 or 1-919-716-6000; and www.ncdoj.gov.

For Rhode Island residents, the Rhode Island Attorney General may be reached at: 150 South Main Street, Providence, RI 02903; www.riag.ri.gov; and 1-401-274-4400. Under Rhode Island law, you have the right to obtain any police report filed in regard to this incident. There are [#] Rhode Island residents impacted by this incident.