

# BakerHostetler

## Baker&Hostetler LLP

811 Main Street  
Suite 1100  
Houston, TX 77002-6111

T 713.751.1600  
F 713.751.1717  
www.bakerlaw.com

William R. Daugherty  
direct dial: 713.646.1321  
wdaugherty@bakerlaw.com

November 19, 2018

### VIA OVERNIGHT MAIL AND EMAIL (CONSUMER@AG.IOWA.GOV)

Consumer Protection Division  
Security Breach Notifications  
Office of the Attorney General of Iowa  
1305 E. Walnut Street  
Des Moines, Iowa 50319-0106

*Re: Incident Notification*

Dear Sir or Madam:

We are writing to notify you of an incident on behalf of our client, Francesca's Services Corporation ("Francesca's").

Francesca's was notified by one of its former third-party vendors, Social Annex, Inc. dba Annex Cloud ("Annex Cloud"), that it had identified and removed unauthorized code that was inserted into Annex Cloud's systems that operate its Social Login application. Annex Cloud's application enables individuals to use their user name and password from social media and other websites, like Facebook and Amazon, to checkout on merchants' websites, including www.francescas.com. Annex Cloud informed Francesca's that they had identified time periods between December 28, 2017 and July 9, 2018 when the unauthorized code was or could have been present. If present, the unauthorized code could have captured information entered during the checkout process, including name, address, email address, Francesca's account password, payment card number, expiration date, and card security code (CVV).

Through November 8, 2018, Francesca's sought additional information from Annex Cloud and its e-commerce platform provider, Kibo Software, Inc., to determine what impact the added code would have and the transactions that might be involved. Annex Cloud supplied additional information about their analysis regarding these periods, including their belief that there are certain times inside these periods when it cannot be determined if the unauthorized code was present. However, Francesca's did not exclude the times within these periods when identifying individuals to notify.

Beginning on November 19, 2018, Francesca's will provide written notifications via United States Postal Service First-Class mail to 798 Iowa residents who entered information during the checkout process during the time periods identified by Annex Cloud. A copy of the notification letter is enclosed. In the notification letters, Francesca's advises individuals to reset the passwords to their Francesca's accounts and

Atlanta Chicago Cincinnati Cleveland Columbus Costa Mesa Denver  
Houston Los Angeles New York Orlando Philadelphia Seattle Washington, DC

for other accounts, if they use the same password, and to monitor their payment card statements for unauthorized charges. Francesca's has also provided a telephone number for individuals to call with any questions they may have. Francesca's is providing notice as soon as possible in compliance with Ia. Code Ann. §§ 715C.1 *et seq.* after working to obtain information needed from Annex Cloud to determine how to identify the individuals to notify.

To prevent this from happening again, Francesca's has removed Annex Cloud's Social Login application from its website.

Please do not hesitate to contact me if you have any questions regarding this matter.

Sincerely,

A handwritten signature in black ink, appearing to read "Will R. Daugherty". The signature is written in a cursive style with a large, sweeping flourish at the end.

Will R. Daugherty

Enclosure



Return Mail Processing Center  
P.O. Box 6336  
Portland, OR 97228-6336

<<Mail ID>>  
<<Name 1>>  
<<Name 2>>  
<<Address 1>>  
<<Address 2>>  
<<Address 3>>  
<<Address 4>>  
<<Address 5>>  
<<City>><<State>><<Zip>>  
<<Country>>

<<Date>>

Dear <<Name 1>>:

Francesca's Services Corporation ("Francesca's") values the relationship we have with our customers and understands the importance of protecting customer information. We are writing to inform you about an incident involving one of our former third-party vendors, Annex Cloud, that previously provided a service only on our website, and which may involve some of your information. This notice explains the incident, measures that have been taken, and some steps you can take in response.

Annex Cloud provides a service used by websites that enables individuals to use their user name and password from other websites, like Facebook and Amazon, to log in to merchants' websites, including [www.francescas.com](http://www.francescas.com). Annex Cloud informed Francesca's that unauthorized code was detected and has since been removed from the code used by Annex Cloud to enable logins. In its report to Francesca's, Annex Cloud identified time periods between December 28, 2017 and July 9, 2018 when the unauthorized code was or could have been present. If present, the unauthorized code could have captured information entered during the checkout process including name, address, email address, Francesca's account password, payment card number, expiration date, and card security code (CVV). Through November 8, 2018, Francesca's sought additional information from Annex Cloud to determine the transactions that might be involved, and Annex Cloud supplied additional information about their analysis regarding these periods, including their belief that there are certain times inside these periods where it is not clear if the unauthorized code was present. Thus, we are notifying you because you entered information during the checkout process during a time period when it is possible the unauthorized code may have been present.

If you have a Francesca's account, for your security, we recommend that you reset your password. Please visit <https://www.francescas.com/account/passwordrecovery.do> and follow the password reset process. Also, if you use the same username and password for any other account, we recommend that you change your password there as well.

We encourage you to closely review your payment card statements for any unauthorized charges. You should immediately report any such charges to the bank that issued your card. If reported timely, payment card network rules generally provide that cardholders are not responsible for unauthorized charges. Information on additional steps you can take can be found on the following pages.

We regret that this incident occurred and apologize for any inconvenience. To help prevent a similar incident from occurring in the future, we have removed the Annex Cloud login feature from our website.

If you have questions, please call 888-510-9591, Monday – Friday, from 8am – 8pm, Central Time.

Sincerely,

A handwritten signature in black ink, appearing to read "E. Li". The letters are stylized and connected.

Erik Lautier

Executive Vice President of Ecommerce and Chief Marketing Officer

## **ADDITIONAL STEPS YOU CAN TAKE**

We recommend that you remain vigilant for incidents of fraud or identity theft by reviewing your account statements and free credit reports for any unauthorized activity. You may obtain a copy of your credit report, free of charge, once every 12 months from each of the three nationwide credit reporting companies. To order your annual free credit report, please visit [www.annualcreditreport.com](http://www.annualcreditreport.com) or call toll free at 1-877-322-8228. Contact information for the three nationwide credit reporting companies is as follows:

*Equifax*, PO Box 740241, Atlanta, GA 30374, [www.equifax.com](http://www.equifax.com), 1-800-685-1111  
*Experian*, PO Box 2002, Allen, TX 75013, [www.experian.com](http://www.experian.com), 1-888-397-3742  
*TransUnion*, PO Box 2000, Chester, PA 19016, [www.transunion.com](http://www.transunion.com), 1-800-916-8800

If you believe you are the victim of identity theft or have reason to believe your personal information has been misused, you should immediately contact the Federal Trade Commission and/or the Attorney General's office in your state. You can obtain information from these sources about steps an individual can take to avoid identity theft as well as information about fraud alerts and security freezes. You should also contact your local law enforcement authorities and file a police report. Obtain a copy of the police report in case you are asked to provide copies to creditors to correct your records. Contact information for the Federal Trade Commission is as follows:

*Federal Trade Commission*, Consumer Response Center, 600 Pennsylvania Avenue, NW Washington, DC 20580, [www.ftc.gov/idtheft](http://www.ftc.gov/idtheft), 1-877-IDTHEFT (438-4338)

**If you are a resident of Connecticut, Maryland, or North Carolina**, you may contact and obtain information from your state attorney general at:

*Connecticut Attorney General's Office*, 55 Elm Street, Hartford, CT 06106 [www.ct.gov/ag](http://www.ct.gov/ag), 1-860-808-5318

*Maryland Attorney General's Office*, 200 St. Paul Place, Baltimore, MD 21202 [www.oag.state.md.us](http://www.oag.state.md.us), 1-888-743-0023 (toll free when calling within Maryland) 1-410-576-6300 (for calls originating outside Maryland)

*North Carolina Attorney General's Office*, 9001 Mail Service Center, Raleigh, NC 27699, [www.ncdoj.gov](http://www.ncdoj.gov), 1-919-716-6400 or toll free at 1-877-566-7226

**If you are a resident of West Virginia**, you have the right to ask that nationwide consumer reporting agencies place "fraud alerts" in your file to let potential creditors and others know that you may be a victim of identity theft, as described below. You also have a right to place a security freeze on your credit report, as described below.

**Fraud Alerts:** There are two types of fraud alerts you can place on your credit report to put your creditors on notice that you may be a victim of fraud—an initial alert and an extended alert. You may ask that an initial fraud alert be placed on your credit report if you suspect you have been, or are about to be, a victim of identity theft. An initial fraud alert stays on your credit report for at least 90 days. You may have an extended alert placed on your credit report if you have already been a victim of identity theft with the appropriate documentary proof. An extended fraud alert stays on your credit report for seven years. You can place a fraud alert on your credit report by contacting any of the three national credit reporting agencies.

**Credit Freezes:** You have the right to put a credit freeze, also known as a security freeze, on your credit file, free of charge, so that no new credit can be opened in your name without the use of a PIN number that is issued to you when you initiate a freeze. A security freeze is designed to prevent potential credit grantors from accessing your credit report without your consent. If you place a security freeze, potential creditors and other third parties will not be able to get access to your credit report unless you temporarily lift the freeze. Therefore, using a security freeze may delay your ability to obtain credit.

There is no fee to place or lift a security freeze. Unlike a fraud alert, you must separately place a security freeze on your credit file at each credit reporting company. For information and instructions to place a security freeze, contact each of the credit reporting agencies at the addresses below:

**Equifax Security Freeze**, PO Box 105788, Atlanta, GA 30348, [www.equifax.com](http://www.equifax.com)  
**Experian Security Freeze**, PO Box 9554, Allen, TX 75013, [www.experian.com](http://www.experian.com)  
**TransUnion Security Freeze**, PO Box 2000, Chester, PA 19016, [www.transunion.com](http://www.transunion.com)

In order to request a security freeze, you will need to provide the following information:

1. Your full name (including middle initial as well as Jr., Sr., II, III, etc.)
2. Social Security number
3. Date of birth
4. If you have moved in the past five years, provide the addresses where you have lived over the prior five years
5. Proof of current address such as a current utility bill or telephone bill
6. A legible photocopy of a government issued identification card (state driver's license or ID card, military identification, etc.)
7. If you are a victim of identity theft, include a copy of the police report, investigative report, or complaint to a law enforcement agency concerning identity theft

The credit reporting agencies have one business day after receiving your request by toll-free telephone or secure electronic means, or three business days after receiving your request by mail, to place a security freeze on your credit report. The credit bureaus must also send written confirmation to you within five business days and provide you with a unique personal identification number ("PIN") or password or both that can be used by you to authorize the removal or lifting of the security freeze.

To lift the security freeze in order to allow a specific entity or individual access to your credit report, or to lift a security freeze for a specified period of time, you must submit a request through a toll-free telephone number, a secure electronic means maintained by a credit reporting agency, or by sending a written request via regular, certified, or overnight mail to the credit reporting agencies and include proper identification (name, address, and Social Security number) and the PIN number or password provided to you when you placed the security freeze as well as the identity of those entities or individuals you would like to receive your credit report or the specific period of time you want the credit report available. The credit reporting agencies have one business day after receiving your request by toll-free telephone or secure electronic means, or three business days after receiving your request by mail, to lift the security freeze for those identified entities or for the specified period of time.

To remove the security freeze, you must submit a request through a toll-free telephone number, a secure electronic means maintained by a credit reporting agency, or by sending a written request via regular, certified, or overnight mail to each of the three credit bureaus and include proper identification (name, address, and Social Security number) and the PIN number or password provided to you when you placed the security freeze. The credit bureaus have one business day after receiving your request by toll-free telephone or secure electronic means, or three business days after receiving your request by mail, to remove the security freeze.

**Fair Credit Reporting Act:** You also have rights under the federal Fair Credit Reporting Act, which promotes the accuracy, fairness, and privacy of information in the files of consumer reporting agencies. The FTC has published a list of the primary rights created by the FCRA (<https://www.consumer.ftc.gov/articles/pdf-0096-fair-credit-reporting-act.pdf>), and that article refers individuals seeking more information to visit [www.ftc.gov/credit](http://www.ftc.gov/credit).

The FTC's list of FCRA rights includes:

- You have the right to receive a copy of your credit report. The copy of your report must contain all the information in your file at the time of your request.
- Each of the nationwide credit reporting companies – Experian, TransUnion and Equifax – is required to provide you with a free copy of your credit report, at your request, once every 12 months.
- You are also entitled to a free report if a company takes adverse action against you, like denying your application for credit, insurance, or employment, and you ask for your report within 60 days of receiving notice of the action. The notice will give you the name, address, and phone number of the credit reporting company. You're also entitled to one free report a year if you're unemployed and plan to look for a job within 60 days; if you're on welfare; or if your report is inaccurate because of fraud, including identity theft.
- You have the right to ask for a credit score.
- You have the right to dispute incomplete or inaccurate information.
- Consumer reporting agencies must correct or delete inaccurate, incomplete, or unverifiable information.
- Consumer reporting agencies may not report outdated negative information.
- Access to your file is limited. And you must give your consent for reports to be provided to employers.
- You may limit "prescreened" offers of credit and insurance you get based on information in your credit report.
- You may seek damages from violators.
- Identity theft victims and active duty military personnel have additional rights.