

July 23, 2019

Dear [NAME REDACTED],

We at Symmetry Partners (“Symmetry”) are writing to share with you some important information regarding an incident involving your personal information at CJS Financial Corp. (“CJS Financial”). You are receiving this letter because your account with CJS Financial appears to have been subject to a fraudulent distribution order.

### **What Happened?**

Beginning on or about March 29, 2019 through and including May 6, 2019, Symmetry received ten email communications that appeared to be from Carl Smith or CJS Financial containing fraudulent transaction requests, regarding six of his customers. No other customers of Symmetry were involved in any way; only customers of CJS Financial were involved. At the time, the requests appeared genuine because they came from a CJS Financial email account and had correct account information as well as the correct E\*Trade custody information; along with an accurate copy of your signature; and so the requests were honored. Subsequently, Symmetry was informed that these requests were fraudulent.

To help understand the situation, Symmetry hired a leading third-party computer forensic expert, Stroz Friedberg, an Aon Company, to review its systems. On June 4, 2019, Stroz Friedberg issued a report concluding that the fraudulent emails were likely sent from CJS Financial’s system, and that Symmetry did not suffer a breach of its email system. Based on this report, our understanding is that Symmetry’s computer system data have not been improperly accessed or compromised.

Unfortunately, we do not have insight into the computer environment at CJS Financial, and they have not agreed to give us access to the relevant logs. Accordingly, your best source of further information about this incident is by contacting CJS Financial by mail at 1 Tara Boulevard, Ste. 200, Nashua NH 03062 or by phone at (954) 825-0309.

### **What Information Was Involved?**

Although the investigation is continuing, we currently believe that a third party may have accessed all of your personal account data held at CJS Financial, including full account information, social security numbers, name, and address. Because any potential compromise of your information did not occur at Symmetry and we do not have access to the files of CJS Financial, we are unable to provide particular information about what information was actually involved.

## **What We Are Doing.**

Beyond having a third-party forensic review of its systems by Stroz Friedberg, Symmetry has contacted the FBI, and we have been working with the Office of the Attorney General of Connecticut and E\*Trade, the custodian of your account, to determine what happened. We understand that E\*Trade is conducting its own independent investigation into the incident and is working to reclaim any fraudulently transferred assets.

We have attempted to coordinate our investigation with CJS Financial, but our efforts to date have not been successful. We are providing you with this notice about the incident to you out of an abundance of caution in case you have not already received notice from CJS Financial.

## **What You Can Do.**

If you receive an email, call or other contact from anyone you do not know requesting sensitive financial information, please do not share your information and let us and law enforcement know immediately.

We strongly encourage you to regularly review your financial accounts and report any suspicious or unrecognized activity immediately. You should remember to be particularly vigilant for the next 12 to 24 months and report any suspected incidents of fraud to the relevant financial institution.

You should in particular review your credit report with care. You are entitled to a free credit report every twelve months from each of the agencies listed below by calling toll free: 1-877-322-8228 or visiting [www.annualcreditreport.com/requestReport/landingPage.action](http://www.annualcreditreport.com/requestReport/landingPage.action).

We regret that this incident occurred, and we hope that efforts to recover the funds are successful.

Sincerely,



**Patrick A. Sweeny**  
Principal and Co-Founder  
Symmetry Partners

**Important Information**  
**Additional Steps You Can Take to Protect Your Identity**

**Review Your Accounts and Credit Reports**

Regularly review statements from your accounts and periodically obtain your credit report from one or more of the national credit reporting companies. You may obtain a free copy of your credit report online at [www.annualcreditreport.com](http://www.annualcreditreport.com) by calling toll free 1.877.322.8228, or by mailing an Annual Credit Report Request Form (available at [www.annualcreditreport.com](http://www.annualcreditreport.com)) to: Annual Credit Report Request Service. P.O. Box 105281, Atlanta, GA, 30348-5281.

You may also purchase a copy of your credit report by contacting one or more of the three national credit reporting agencies listed below:

- **Equifax**, P.O. Box 740241, Atlanta, Georgia 30374-0241.  
Toll free: 1-800-685-1111. [www.equifax.com](http://www.equifax.com)
- **Experian**, P.O. Box 9532, Allen, TX 75013.  
Toll free: 1-888-397-3742. [www.experian.com](http://www.experian.com)
- **TransUnion**, 2 Baldwin Place, P.O. Box 1000, Chester, PA 19016.  
Toll free: 1-800-916-8800. [www.transunion.com](http://www.transunion.com)

**Consider Placing a Fraud Alert**

You may wish to consider contacting the fraud department of the three major credit bureaus to request that a “fraud alert” be placed on your file. A fraud alert notifies potential lenders to verify your identification before extending credit in your name, so creditors may take extra steps to validate your identity before opening a new account or changing your existing accounts (for that reason, it may delay obtaining credit).

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. An initial fraud alert is free and stays on your credit report for at least one year. 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.

<b>Equifax:</b>	Report Fraud:	1-800-525-6285
<b>Experian:</b>	Report Fraud:	1-888-397-3742
<b>TransUnion:</b>	Report Fraud:	1-800-680-7289

## Consider a Security Freeze with the Credit Reporting Agencies

You may wish to request a security freeze on your credit reports. A security freeze prohibits a credit reporting agency from releasing any information from a consumer's credit report without written authorization. However, please be aware that placing a security freeze on your credit report may delay, interfere with, or prevent the timely approval of any requests you make for new loans, credit mortgages, employment, housing or other services. It is free to place, lift or remove a security freeze.

Unlike a fraud alert, you must separately place a security freeze on your credit report at each credit bureau. To do so, you must contact the credit bureaus by phone, mail, or secure electronic means:

- **Equifax:** P.O. Box 105788, Atlanta, GA 30348, 1-800-349-9960, [www.Equifax.com](http://www.Equifax.com)
- **Experian:** P.O. Box 9554, Allen, TX 75013, 1-888-397-3742, [www.Experian.com](http://www.Experian.com)
- **TransUnion:** P.O. Box 160, Chester, PA 19106, 1-888-909-8872, [www.TransUnion.com](http://www.TransUnion.com)

To request a security freeze, you will need to provide the following:

- Your full name (including middle initial, Jr., Sr., Roman numerals, etc.),
- Social Security number
- Date of birth
- Address(es) where you have lived over the prior five years
- Proof of current address such as a current utility bill
- A photocopy of a government-issued ID card
- If you are a victim of identity theft, include a copy of either the police report, investigative report, or complaint to a law enforcement agency concerning identity theft

If you request a freeze online or by phone, the agency must place the freeze within one business day. The credit bureaus have three business days after receiving a request by mail to place a security freeze on your credit report, and they must also send 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 freeze to allow a specific entity or individual access to your credit report, you must contact the credit reporting agencies and include (1) proper identification; (2) the PIN number or password provided to you when you placed the security freeze; and (3) the identities 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.

## Know Your Fair Credit Reporting Act Rights

You also have rights under the federal Fair Credit Reporting Act ("FCRA"), which promotes the accuracy, fairness, and privacy of information in the files of consumer reporting agencies. The FTC has information about the primary rights created by the FCRA (<https://www.consumer.ftc.gov/articles/pdf-0096-fair-credit-reporting-act.pdf>). That

The FTC's list of FCRA rights includes:

- (1) you must be told if information in your file has been used against you;
- (2) you have the right to know what is in your file;
- (3) you have the right to ask for a credit score;
- (4) you have the right to dispute inaccurate information;
- (5) consumer reporting agencies must correct or delete inaccurate, incomplete or unverifiable information;
- (6) consumer reporting agencies may not report outdated negative information;
- (7) access to your file is limited;
- (8) you must give your consent for reports to be provided to employers;
- (9) you may limit "prescreened" offers of credit and insurance you get based on information in your credit report;
- (10) you have a right to place a security freeze on your credit report and fraud alert on your credit file;
- (11) you may seek damages from violators; and
- (12) identity theft victims and active duty military personnel have additional rights.

### Suggestions if You Are a Victim of Identity Theft

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 FTC, the Attorney General's office in your state and/or local law enforcement – they can provide information about preventing identity theft.

- **File a police report.** You also have the right to file and obtain a police report regarding this incident. Get a copy of the report to submit to your creditors and others that may require proof of a crime.
- **Contact the U.S. Federal Trade Commission (FTC).** The FTC provides useful information to identity theft victims and maintains a database of identity theft cases for use by law enforcement agencies. File a report with the FTC by:
  - calling the FTC's Identity Theft Hotline: 1-877-IDTHEFT (438-4338)
  - online at <http://www.ftc.gov/idtheft>; or
  - by mail at Identity Theft Clearinghouse, Federal Trade Commission, 600 Pennsylvania Ave., N.W., Washington, DC 20580.
 Also request a copy of the publication, "Take Charge: Fighting Back Against Identity Theft" from <http://www.ftc.gov/bcp/edu/pubs/consumer/idtheft/idth04.pdf>.
- **Keep a record of your contacts.** Start a file with copies of your credit reports, the police reports, any correspondence, and copies of disputed bills. It is helpful to log conversations with creditors, law enforcement officials, and other relevant parties.



151 National Drive | Glastonbury, CT 06033 | 860.734.2000 | [symmetrypartners.com](http://symmetrypartners.com)

### **Take Steps to Avoid Identity Theft**

Further information can be obtained from the FTC about steps to take to avoid identity theft at: <http://www.ftc.gov/idtheft>; calling 1-877-IDTHEFT (438-4338); or write to Consumer Response Center, Federal Trade Commission, 600 Pennsylvania Ave., N.W., Washington, DC 20580.