MEMORANDUM FROM POLICE DEPARTMENT

DATE: January 8, 2024

TO: CTC Students, Staff, and Faculty

FROM: Joseph A. Barragan, Chief of Police, Security Services

SUBJECT: Timely Warning – Identity Theft / Fraud Guidance for Potential Victims

TIMELY WARNING 2024-0108:

This timely warning to all Central Texas College students, staff, faculty, and community members on all campuses and remote sites is issued to comply with the federal Jeanne Clery Disclosure of Campus Security Policy and Campus Crime Statistics Act (Clery Act) and CTC policies for compliance with that act.

Central Texas College Police Department has become aware of a phishing email that may expose students, staff, and faculty to potential abuse and exploitation. Do not respond to any email requesting you to apply for an "INTERN RESEARCH ASSISTANT" position. These malicious scammers are targeting CTC Email Accounts to commit identity theft and/or fraud. For further information or resources please contact the Police Department at (254) 526-1427.

Victim Assistance: Lessons From the Field*

Tools/Resources for Victims

Steps for Victims of Identity Theft or Fraud

If you are a victim of identity theft remember that when dealing with the authorities and financial institutions, it is very important to keep a log of all conversations, including dates, names, and phone numbers. Be sure to note time spent and any expenses incurred, in case you are able to request restitution in a later judgment or conviction. Make sure you confirm conversations in writing and send all correspondence by certified mail, return receipt requested. Keep copies of all letters and documents.

- **Place a fraud alert on your credit report**.
- **Close out accounts that have been tampered with or opened fraudulently**.
- **Report the identity theft to the Federal Trade Commission**.
- **File a report with your local police department**.

Place a fraud alert on your credit report. Fraud alerts can help prevent an identity thief from opening any more accounts in your name. Contact the toll-free fraud telephone number of any of the three consumer reporting agencies (CRAs) below to place a fraud alert on your credit report. You need only contact one of the three CRAs to place an alert. That company is required to contact the other two, which will place alerts on their

versions of your report, too. If you do not receive a confirmation from a company, you should contact that company directly to place a fraud alert.

Once you place the fraud alert in your file, you're entitled to order one free copy of your credit report from each of the three CRAs, and, if you ask, only the last four digits of your Social Security number will appear on your credit reports. Once you get your credit reports, review them carefully. Look for inquiries from companies you haven't contacted, accounts you didn't open, and debts on your accounts that you can't explain. Check that information like your Social Security number, address(es), name or initials, and employers are correct. If you find fraudulent or inaccurate information, get it removed.

Continue to check your credit reports periodically, especially for the first year after you discover the identity theft, to make sure no new fraudulent activity has occurred.

Consumer Reporting Agencies (CRA's)

1. **Equifax**
   P.O. Box 740241, Atlanta, GA 30374-0241
   Phone: 800-525-6285
   Web site: **www.equifax.com**

2. **Experian**
   P.O. Box 9701, Allen, TX 75013-0949
   Phone: 888-397-3742
   Web site: **www.experian.com**

3. **TransUnion**
   P.O. Box 6790, Fullerton, CA 92834
   Phone: 800-680-7289
   Web site: **www.transunion.com**

Back To Top

Close the accounts that you know or believe have been tampered with or opened fraudulently. Call and speak with someone in the security or fraud department of each company. Follow up in writing and include copies (NOT originals) of supporting documents. It's important to notify credit card companies and banks in writing. Send your letters by certified mail, return receipt requested, so you can document what the company received and when. Keep a file of your correspondence and enclosures.

When you open new accounts, use new personal identification numbers (PINs) and passwords. Avoid using easily available information like your mother's maiden name, your birth date, the last four digits of your Social Security number or your phone number, or a series of consecutive numbers.

If the identity thief has made charges or debits on your accounts or has fraudulently opened accounts, ask the company for the forms to dispute those transactions. For charges and debits on existing accounts, ask the representative to send you the company's fraud dispute forms. If the company doesn't have special forms, use the FTC's **sample letter** to dispute the fraudulent charges or debits. In either case, write to the company at the address given for "billing inquiries," NOT the address for sending your payments.

For new unauthorized accounts, you can either file a dispute directly with the company or file a report with the police and provide a copy, called an "Identity Theft Report," to the company.

If you want to file a dispute directly with the company and do not want to file a report with the police, ask if the company accepts the FTC's **ID Theft Affidavit** (PDF, 56 kb). If it does not, ask the representative to send you the company's fraud dispute forms.

The statutory procedures for disputing fraudulent accounts and clearing credit reports are not easy to follow, and if a victim fails to follow the procedure to the letter, then he or she may not get the help needed. VICARS attempted to distill the statutory procedures into a series of steps that could be followed in sequence. This **consumer guide** (PDF 2 mb) contains contact information for relevant law enforcement agencies, federal and state agencies, and other identity theft programs such as those offered by the grantees.

Filing a report with the police and then providing the company with an Identity Theft Report, however, will give you greater protection. For example, if the company has already reported these unauthorized accounts or debts on your credit report, an Identity Theft Report will require them to stop reporting that fraudulent information. Use the **cover letter** to explain to the company the rights you have by using the Identity Theft Report.

Once you have resolved your identity theft dispute with the company, ask for a letter stating that the company has closed the disputed accounts and has discharged the fraudulent debts. This letter is your best proof if errors relating to this account reappear on your credit report or you are contacted again about the fraudulent debt.

Back To Top

Report the theft to the Federal Trade Commission. The FTC will not investigate your case, but after making a report, it will enter your information into the **Identity Theft Data Clearinghouse**, a nationwide databank that assists law enforcement in the investigation and prosecution of identity thieves. You can **file a complaint online** with the FTC. If you don't have Internet access, call the FTC's Identity Theft toll free hotline at 1-877-IDTHEFT (1-877-438-4338).

Back To Top

File a police report. When you speak to your local police department about filing your report, have a printed copy of your ID Theft Complaint form, your **cover letter**, and your supporting documentation. The cover letter explains why a police report and an ID Theft Complaint are so important to victims. (Additional instructions for **filing a complaint form**.)

Ask the officer to attach or incorporate the ID Theft Complaint into his or her police report. Tell the officer that you need a copy of the Identity Theft Report (the police report with your ID Theft Complaint attached or incorporated) to dispute the fraudulent accounts and debts created by the identity thief.

What do I do if the local police won't take a report? There are efforts at the federal, state, and local level to ensure that local law enforcement agencies understand identity theft, its impact on victims, and the importance of taking a police report. However, we still hear that some departments are not taking reports. The following tips may help you to get a report if you're having difficulties:

- Provide the officer with a copy of the **Law Enforcement Cover Letter** that explains why the police report and the Identity Theft Report are so important to both victims and industry.

- Furnish as much documentation as you can to prove your case. Debt collection letters, credit reports, a copy of your printed ID Theft Complaint, and other evidence of fraudulent activity can help demonstrate the legitimacy of your case.

Be persistent if local authorities tell you that they can't take a report. Stress the importance of a police report; many creditors require one to resolve your dispute. Remind them that consumer reporting companies will automatically block the fraudulent accounts and bad debts from appearing on your credit report, but only if you can give them a copy of the police report. In addition, a police report may be needed to **obtain the fraudulent application** and other records the company has.

SOURCE*:

Expanding Services To Reach Victims of Identity Theft and Financial Fraud - Victim Assistance: Lessons From the Field - Steps for Victims of Identity Theft or Fraud (ojp.gov)

HELPFUL RESOURCE LINKS:

https://consumer.ftc.gov/articles/what-know-about-identity-theft

https://www.texasattorneygeneral.gov/consumer-protection/identity-theft/what-do-if-your-identity-stolen

https://www.usa.gov/identity-theft

https://ovc.ojp.gov/sites/g/files/xyckuh226/files/pubs/ID_theft/serviceprovider.html

https://www.ic3.gov/

https://www.usbank.com/financialiq/manage-your-household/protect-your-assets/identity-stolen-5-steps-to-take-immediately.html