AUGUSTIN LAW OFFICES, PLLC

Ernscie Augustin is an attorney with the firm and Ingham County Public Administrator. Ms. Augustin serves as a board member of the Ingham County Bar Association, the Elder Law Advisory Board, and the State Bar of Michigan Probate Council. She is chair of the Ingham County Bar Association's Probate and Trust Section, a member of the Greater Lansing Estate Planning Council, the Michigan State University Inn of Court and Rotary Club of Lansing. Ms. Augustin was the 2024 Super Lawyers- Michigan Rising Star Award, 2023 recipient of the Ingham County Bar Association's President's Award, Best Lawyers: Ones to Watch in America, 2020 Ingham County Bar Association's "Top 5 Under 35" Award, and the 2019 Davis Dunnings Bar Association Rising Star Award.

Client Handout For A Victim Of A Financial Scam

Financial scams are on the rise and financial scammers are becoming more sophisticated. Elderly individuals are often targeted due to their vulnerability. An elderly client may come to you alone or with a family member for advice for potential remedies. These cases can be difficult for a client to recover from, especially when it's an unidentifiable/unknown scammer and they also have to deal with financial institutions' regulations.

1. **Report the financial scam within 2-3 days** to the police or prosecutors' office. Provide them with detailed information regarding the incident and file a police report. Call the National Elder Fraud Hotline at 833-FRAUD-11 to obtain assistance. The hotline will identify appropriate reporting agencies, and provide information to callers to assist them in reporting, or connect callers directly with the appropriate agency.

2. **Review the transaction history on your accounts and immediately notify financial institutions** of suspicious transactions. and request they either freeze your account or replace your bank card, depending upon your situation. Take detailed notes when communicating with your bank, including the name and

contact information of the representative who is assisting you. Inquire about options to reverse fraudulent charges or to file a complaint regarding unauthorized transactions.

3. **Obtain information on how your financial institution alerts customers** and how they require customers to respond. Scammers have been known to send fake alerts with a code and to call their targets about the scam incident while posing as the target's financial institution, which can be very believable. If you provide the scammer with the code, they may be able to utilize this information to remove additional funds from your account. It's good practice to independently look up your financial institution's phone number and call them, or visit them in person, if you receive an unexpected alert. Most financial institutions will never ask you to provide a texted security code over the phone.

4. **Set instant alerts** so your financial institution will call, email, or text notifications of transactions as they occur. Be sure to regularly review your alerts and bank statements.

5. **Change your passwords** so scammers cannot continue to access your financial accounts. If you were targeted on your mobile or computer device, you should update your password so that scammers are unable to access your device remotely. Set up any security measures available for your accounts, including two-step verification or security questions. These measures deter a scammer from accessing your accounts as you will be alerted if someone attempts to access your account with the incorrect code or security question answers.

6. **Contact the credit bureaus** and request either a credit lock, credit freeze, or fraud alert. A credit lock allows you to control who can view your credit report, but may incur a fee. A credit freeze can keep unauthorized people from accessing your credit file, which helps deter identity thieves from opening accounts in your name, but doesn't completely block access to your file and creditors you already have a relationship with and/or government agencies that are executing court orders, subpoenas, or search warrants can still access it. A fraud alert is a notation on your credit report that requires creditors and lenders to verify your identity before approving new lines of credit in your name, but doesn't completely lock down your credit report. Additionally, check your credit score to see if the unauthorized transactions affected your score. The contact information for the credit bureaus is:

a. **Equifax** – www.equifax.com – 1-888-685-1111
b. **Experian** – www.experian.com – 1-888-397-3742
c. **TransUnion** – www.transunion.com – 1-800-909-8872

7. **Save a copy of the correspondence** that led to the scam, whether it is mail, email, text messages, or phone number. Pursuing claims against scammers is difficult, but a paper trail may be useful for your attorney, financial institutions, and loved ones.

8. **Advise your loved ones** of the incident. Do not be ashamed or embarrassed to discuss this. Perhaps you shared sensitive information regarding your loved ones, or the scammer discovered the information. It's important to notify them in case they are targeted. Additionally, if your loved one manages your finances as your power of attorney, conservator, or trustee, it would be important for them to know.

9. **Do not share additional sensitive information.** Sometimes scammers may attempt to contact you again a different way. They might impersonate a company or an individual to pressure you to immediately send more money. Do not share additional information with them no matter how friendly they are or how trivial the information requested.