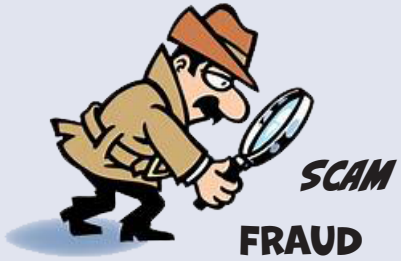
HELPFUL TIPS:

- Report any phone calls, mail, or emails that are suspected scams to the local New York State Attorney General's Office at **(716) 853-8400**.
- Use passwords that include numbers, characters and punctuation. Never use personal information (birthdates, addresses, etc.) Do not use the same password for ***ALL*** accounts.
- Information on COVID-19 related scams can be found at www.ftc.gov/coronavirus/scam-consumer-advice.
- If you have a payment issues or think you may owe additional taxes, call the Internal Revenue Service directly at **1-800-829-1040**.
- The New York State Department of Financial Services can be reached at **1-(800) 342-3736** or via the internet at their website: **www.dfs.ny.gov.** Here, you can verify a variety of state licensures for different professions.
- Information on other scams and what to do can be found by scanning the QR code below.



Comptroller Hardwick and his family moved to the City of Tonawanda in 1989 when he accepted a job in the Political Science Department at Canisius College.

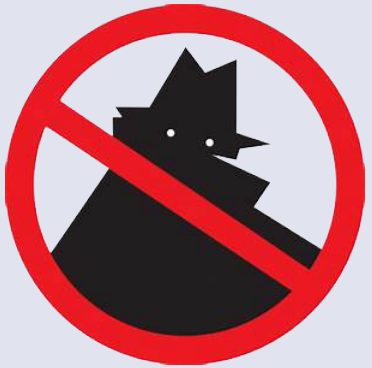
He is a former chair of the Political Science Department and currently serves as the Director of the Urban Studies Program.
In 2009 he was elected to the Erie County Legislature representing Grand Island and the Tonawandas. He was re-elected five times.
In 2021, he was elected Erie County Comptroller for the term commencing in 2022.

Office of The Erie County Comptroller
95 Franklin Street ▪ 11th Floor
Buffalo, NY 14202

(716)858-8400

Comptroller@Erie.gov

Whistle Blower Hotline:
(716)858-7722



2022 SCAM/FRAUD PREVENTION

Serving taxpayers while protecting Seniors

Presented by:
Erie County Comptroller
Kevin Hardwick

TOP SCAMS TARGETING OLDER ADULTS:

Zoom phishing emails:
Texts, emails or social media with the Zoom logo asking you to click a link because you missed a meeting. Zoom's real website is "Zoom.us" and refers to customer support.

Fake online shopping websites:
Click on an online ad that mimics real online retailers to get credit card information.

Online romance scams:
Scammers lure people off monitored sites onto less monitored sites like: Google Hangouts, WhatsApp, Facebook Messenger and eventually hit you up for money or gift cards. If you suspect a romance scam, cut off contact immediately and report to it to **www.ftc.gov/complaint**. If you met through a dating site, notify the site immediately.

Medicare card scams:
You may receive an email, phone call or a knock on the door from someone claiming to be from Medicare offering services if you ***"verify"*** the Medicare ID number.

Peer to peer (P2P) payment scams:
With new smart phone tools that let you transfer money directly to another person like Venmo, Zelle, PayPal and CashApp, scammers will transfer funds into bank accounts then send a follow up message requesting the funds be transferred back.

Social Security call scams:
You receive a "spoof" phone call saying you'll be arrested soon because your Social Security # is linked to a crime unless you send money **NOW**!

IRS scams:
Callers may request payment for money via wire transfer or preloaded debit cards/gift cards.

OTHER RESOURCES:

Erie County Department of Health:

Erie County Department of Senior Services:

For City of Buffalo related issues, call 3-1-1 or visit buffalony.gov.

Do Not Call Registry:
1-(888) 382-1222

Identity Theft Hotline:
1-(877) 438-4338

"Fraud" and "scam" are used interchangeably to refer to financial wrongdoing.
Fraud is usually a more serious crime. Scams are one type of fraud.

AVOID BECOMING A VICTIM:

- If you receive unsolicited emails, texts or social media messages: **NEVER** click on links.
- Never click on an ad to go to a retailer's website and check online reviews if you are unfamiliar with the website. Bookmark the URLs of websites you use regularly.
- If it is someone you have haven't met, **NEVER** send money. Don't post or send selfies or videos, especially those that can be used for identity theft or blackmail.
- Medicare will not call to sell you anything *(Covid -19 vaccines are free)*. Permission must be granted, otherwise Medicare will **NOT** contact you. Delete the email, hang up the phone, shut the door. You are not being rude.
- Any funds deposited to your account ***"in error"*** will subsequently be removed from your account. More than likely the scammer used stolen debit cards to make the deposit.
- Don't answer phone calls from numbers that are unknown to you. They will leave a voicemail, if it is important. Scammers always have a sense of urgency.
- The IRS initiates contact through mail. The IRS does not request personal, financial or credit card information through email or over the phone.