Testimony Offered to the Senate Banking and Insurance and Aging and Youth Committees' Joint Public Hearing on Elder Financial Abuse Prevention and Response (HB 2064) September 18, 2024

Good morning, Chairmen DiSanto, Street, Ward and Collett and Committee members. We are Rick Cimakasky, Vice President of Fraud and Security Management, Penn Community Bank on behalf of the PA Bankers Association; Amey Sgrignoli, CEO of Belco Community Credit Union and Roger Zacharia, Ambler Savings Bank. Our associations have been working together for some time on the important issue before you today.

Background on Elder Financial Exploitation

Elder financial exploitation is the illegal or improper use of an older adult's funds, property, or assets. This includes misuse of powers of attorney, unauthorized withdrawals, scams, check, debit and credit card fraud. Each year, millions of older Americans suffer billions in losses due to financial exploitation, much of which is irrecoverable. Despite its prevalence, quantifying the impact is challenging. The Federal Trade Commission FTC) reported that in 2021 it received 567,340 fraud reports involving adults 60 years of age and older, involving average losses of $820 for individuals ages 60 to 69; $800 for individuals ages 70 to 79, and $1.500 for individuals over 80 years of age.[1] The National Institute of Justice also reported that in 2017, 929,570 older adults were victims of financial fraud, and suffered total losses of $1.2 billion, or an average of $1,270 per-person.[2] With as few as 1 in 44 cases being officially reported, however, it is believed that as many as 1 in 5 seniors may have been victims of a financial swindle.[3]

Overall, both the FTC and the NIJ report that older adults are not more likely than younger persons to report suspected financial exploitation and are more likely than younger persons to take action to avoid losses. Older adults, however, are more susceptible than younger persons to certain types of frauds and swindles, especially those involving tech support; prizes, sweepstakes and lotteries; and exploitation by family members and friends. In comparison to older adults, younger persons are more frequently victims of fraud involving investments, on-line shopping, fake checks, vacation and travel, and romance.

Victims not only suffer financial harm but also endure emotional distress, facing the loss of their savings, homes, and dignity.[4] The impact extends to family caregivers and taxpayers who shoulder additional burdens to support financially devastated victims. As our nation undergoes a demographic shift, with more seniors than children projected within the next decade, the urgency to address elder financial exploitation grows.

---

[1] https://www.ftc.gov/system/files/ftc_gov/pdf/P144400OlderConsumersReportFY22.pdf.
[2] https://nij.ojp.gov/topics/articles/examining-financial-fraud-against-older-adults.
[3] https://www.prnewswire.com/news-releases/survey-1-out-of-5-older-americans-are-financial-swindle-victims-manyadult-children-worry-about-parents-ability-to-handle-finances-96395079.html
[4] The Thief Who Knows You: The Cost of Elder Exploitation Examined (aarp.org)

Financial Industry Measures to Protect Older Adults

Our Associations in collaboration with their national counterparts have spearheaded the development of numerous free tools and resources aimed at educating and increasing awareness about elder financial exploitation. The Safe Banking for Seniors program has been embraced by more than 1600 banks, offers comprehensive materials for conducting in-person or virtual workshops, leveraging social media platforms, and engaging in one-on-one conversations to educate communities about scams and financial protection.[5]

Our industry has also teamed up with the Federal Trade Commission to develop infographics addressing scams targeting seniors. These materials are freely accessible covering topics such as fake check scams, government imposter scams, and romance scams. Additional, ongoing partnerships with organizations like the National Adult Protective Services Association and National Sheriffs Association work towards enhancing communication between banks and state authorities.

The American Bankers Association promotes an acclaimed anti-phishing campaign #BanksNeverAskThat to provide real-world tips for consumers to identify and avoid falling victim to phishing attempts. The campaign covers a wide range of topics, including recognizing suspicious emails, avoiding sharing sensitive information online, and understanding how to spot fraudulent messages. Banks Never Ask That is a vital effort to promote online safety and security for consumers. This campaign is being refreshed for a re-launch of new resources next month.

In addition to providing educational resources, 99% of surveyed banks offer training on elder financial exploitation for frontline staff.[5] Financial institutions actively protect older customers by utilizing automated monitoring tools to detect unusual account activity. When exploitation is suspected, banks promptly assign staff to review accounts and take necessary actions, such as filing suspicious activity reports or flagging and closing accounts.

Legislative Opportunity to Combat Elder Financial Exploitation

While universal bank practices include employee fraud detection training and reporting suspicious activity to the federal government, there is room for improved collaboration between financial institutions and adult protective services. The 2018 approval of the federal Senior Safe Act granted legal immunities to trained bank employees who report elder financial exploitation, resulting in increased reporting to adult protective services. In addition, state legislatures are enacting laws to facilitate greater information sharing and allow for banks to decline to engage in suspicious transactions before irreversible disbursements occur.

Our Associations supported the introduction of HB 2064 to establish a clear legal framework for financial institutions to take actions that will help protect older adults from financial exploitation. The legislation:

- Requires financial institutions to report suspected or attempted financial exploitation of older adults to area agencies on aging when individuals are the targets of exploitation because of their age, infirmity or dependency and in circumstances in which the agencies are able to investigate and provide relief from the exploitation;

[5] https://www.aba.com/news-research/analysis-guides/older-americans-benchmarkingreport#:~:text=More%20than%20half%20of%20the,offer%20such%20products%20(67%25).

- Authorizes financial institutions to include with reports of suspected or attempted financial exploitation financial records to document the basis for reports and help area agencies on aging investigate reports;
- Makes additional financial records needed to investigate reports available to area agencies on aging upon request without the need for consent by an older adult or court order;
- Permits financial institutions to notify a trusted contact associated with the older adult (if available) to assist the older adult;
- Authorizes area agencies on aging to consult with financial institutions filing report on how best to respond to suspected incidents of financial exploitation;
- Provides financial institutions the authority to delay suspicious transactions for further investigation; and
- Protects financial institutions and their employees from civil and criminal liability for filing reports, providing financial records to area agencies on aging, consulting with trusted contacts, and delaying suspicious transactions.

Such legislation would equip institutions with more proactive tools to protect our seniors.

Detrimental Customer Impact of HB 2064 as it Currently Reads

While HB 2064 began as an effort to provide financial institutions better tools to prevent and respond to elder financial exploitation, **it was amended in the House to include to include draconian penalties and increase financial institution liability that could be avoided only by financial institutions' imposing delays on many transactions frustrating older adult customers and those with whom they seek to do business and exposing the institutions to allegations of age discrimination and flooding Area Agencies on Aging with reports**.[6]

In addition, HB 2064 was amended to make banks, credit unions, investment advisors, broker dealers and insurance companies and agents mandatory reporters but excludes all other types of money service businesses, including money transmitters, cryptocurrency exchanges, mortgage brokers, originators and services, check casers, debt management and settlement companies, credit services and loan and consumer discount companies which are experiencing an increasing share of financial exploitation incidents. Although we are prepared to accept mandatory reporting responsibilities, we believe **mandatory reporting should focus on the types of incidents for area agencies on aging are well suited to provide meaningful assistance**, such as incidents involving older adults with diminished capacities and incidents involving family members, guardians, agents holding powers of attorney, and caregivers. As is the practice in most states that impose mandatory reporting requirements on financial institutions, **Pennsylvania should not impose monetary penalties or damage remedies for good faith failures to file reports**, and instead agencies with examination responsibility over financial institutions should be relied upon to take appropriate action to address failures to effectively identify and report suspected financial exploitation of older adults.

[6] Section 606 imposes $10,000 civil penalties for every failure to promptly identify and report suspected financial exploitation, plus damages of up to $250,000 (or $500,000 for joint accounts) on financial institutions that do not block transactions that the institution should have suspected were induced by fraud. The standard of proof for such claims is low. This liability is not recognized in the law of any other state and penalizes institutions even when they are making sincere efforts to detect elder fraud. Additionally, section 607 lowers the level of immunity from civil suits and criminal liability offered by current law for good faith efforts to identify and report suspected financial exploitation, exposing financial institutions to increased legal risk when addressing elder fraud cases.

We should also note that no other state imposes penalties on financial institutions remotely like those in HB 2064. An attempt to impose such penalties on national banks would likely be subject to challenge on the grounds of National Bank Act preemption. If PA's statute were deemed to be preempted with regard to national banks that would significantly reduce the competitiveness of state-chartered banks operating in this Commonwealth.

Our Associations remain committed to combatting elder financial exploitation and welcome a reasonable compromise that fosters collaboration among financial institutions, protective services and law enforcement to enhance the well-being of our seniors; thus, we cannot support HB 2064 as it currently reads and look forward to working with you to restore its original purposes.

Witnesses' Perspectives and Conclusion

I [Rick Cimakasky] served as an FBI Special Agent and now serve as Penn Community's Bank Fraud and Security Officer. I served as an FBI Special Agent and now lead's fraud prevention and loss mitigation efforts for Penn Community Bank as Fraud and Security Officer. Based in Bucks County and serving communities across Bucks, Montgomery, Lehigh, Northampton, and Philadelphia, Penn Community Bank is the largest independent mutual bank in eastern Pennsylvania with over $2.9 billion in assets, 300+ employees, and more than 20 branch and office locations throughout the region. I am here today on behalf of the Pennsylvania Bankers Association and its 117 members of all sizes operating throughout the Commonwealth.

During my time with the FBI, I often found myself consoling elderly victims who had lost their life's savings to fraudsters operating overseas who felt safe from prosecution as we had no mutual legal assistance treaties in place to cooperate with our investigative efforts. Most of these scams related to things like "foreign lotteries" or a romance related fraud involving a fictional military officer deployed overseas. Still in most instances my connection to that victim ended after intake of the complaint.

As a banker, I have witnessed the devastation caused by these schemes far too often. We're often the first to discover and investigate fraud, counsel our customers, and advocate for recovery. Unfortunately, restitution is rare due to the rapid and untraceable nature of international digital currency transfers, preferred by fraudsters.

In contrast to my previous role, where my involvement ended after intake, my current job extends for weeks, or even months. We work tirelessly to prevent further loss, support victims and their families as they work with law enforcement and utilize all available resources in search of recovery options.

I can attest that the criminal organizations that are currently leading the charge at defrauding our Commonwealth's older adults use some of the most well written cover stories, and recruitment techniques that when supported by advanced technology, can easily convince their elderly victims that they are someone they truly are not - such as a computer support customer service associate, the Internal Revenue Service, the County Sheriff's office, or even me, the Fraud and Security Officer for Penn Community Bank. Often, these victims have been communicating with the fraudsters for days. During this time, they have been convinced and coached to lie to their bank and family about their need to withdrawal or transfer funds. To further complicate matters, they are influenced to make no contact with law enforcement, to never trust the bank employees, and keep their cell phones on and monitored by the scammers when entering and communicating with their financial institution during these withdrawals and transfers.

In the past four years, I've witnessed elderly victims of these crimes experience severe consequences, including attempted suicide, family alienation, and the need to return to work to cover basic expenses.

PA Bankers and the banking industry are fully committed to safeguarding our elderly customers from financial exploitation. I can personally confirm the earlier mentioned statistics highlighting the vast threat of this issue. As a result, we prioritize employee training, account monitoring techniques, and engage in educational programs, public awareness campaigns, and advocate for stronger protection measures.

I [**Roger Zacharia**] am president and CEO of Ambler Savings Bank. We have branches in Ambler, Fairview Village, Limerick and Schwenksville. Ambler Savings has been in operation since 1874. We began our mission by providing affordable home financing.

I am also a member of PACB-the Pennsylvania Association of Community Bankers. PACB represents the interests of community banks headquartered throughout Pennsylvania.

Community banks are on the front lines in trying to prevent the financial abuse of older Pennsylvanians. We see, in real time, the devastation that financial fraud against the elderly creates.

That's why in January 2023, we approached Governor Shapiro and legislative leaders about working together on legislation to allow banks to report suspected cases of financial crimes against the elderly.
On a daily basis we see all kinds of attempts to steal hard earned money from seniors. The stories are legion- and disturbing. I will share a few of them now.

One elderly customer stated she received a pop-up on her home computer that said "do not turn your computer off, your social security number was compromised. Call this number ASAP." She was then instructed to withdraw money from her account and deposit it into a Bitcoin ATM machine. She did and lost thousands of her savings. A 77-year-old customer fell victim to bad actors who obtained their personal information then used that information to threaten the customer into sending them $30,000 in cash. The customer would not initially disclose the purpose of the withdrawals even after repeated attempts from bank personnel to obtain the information. An 83-year-old customer came into multiple bank branches attempting to withdraw $30,000 to $40,000 in cash to pay contractors for work they were doing. The customer was questioned and counseled on scams but was withholding information about the company he was working with and was insistent on taking the funds from his account in cash.

Community banks in PA live by one motto-know your customer. Our goal places a strong emphasis on relationships and goes beyond transactional interactions. Our employees become familiar with our customers and their families, their accounts and their patterns-they are truly the first line of defense for our vulnerable senior population. Customer education and awareness is an important tool in the detection and prevention of elder financial abuse. We also consistently provide our customers with educational material to help them recognize the signs of fraud and how to get help.

Community banks spend millions on continuous staff education and training to prevent fraud. Employees receive regular training on how to spot activity that is unusual for members and bank staff ask questions of our customers concerning their transaction history and the purpose of the transactions that they are trying to conduct.
We, as community banks, use every tool we have in our tool box to prevent fraud and harm to seniors but we need a few additions from you, the General Assembly, in order to do our jobs as best as we can and protect our customers-your constituents.

Due to the trusting nature of the elder population, we often struggle with getting the customer to understand how these scams work, as they fully believe the person that they are speaking to is legitimate. Even customers who have banked with us for years will often refuse to heed our warnings.
In order to protect our vulnerable seniors, we need the ability to place holds on transactions that appear to be fraudulent. In order to hold those transactions, we need a safe harbor (immunity) in order to hold a possible fraudulent transaction. We also need the ability to not hold a transaction if it's legitimate. Our banks report to the Area Agency on Aging (AAA) but we don't receive any follow up as to the result. This is not a criticism, merely an experienced observation. We need feedback to better prevent fraud the next time.

Banks need the ability to report apparent fraudulent transactions without the fear of violating privacy laws. Let us exercise sound judgement and experience in combating fraud. Let those closest to the transaction, and with the expertise, make the decision. Otherwise, legitimate business customer activity will be thwarted.

The goal of HB 2064 is noble-protecting seniors from financial exploitation. However, as amended in the House, HB 2064 may cause more problems than it solves.

The unintended consequence of HB 2064 in its current form would force a bank or credit union to hold every transaction for a person 60 and older out of fear that not doing so would result in substantial penalties and civil liability. At the same time, banks or credit unions holding transactions for persons over 60 would be subject to discrimination claims under the federal Americans with Disabilities Act. Finally, reporting suspicious activity on a bank customer's account subjects banks and credit unions to liability for violating privacy.

Rather than imposing substantial penalties and creating new liabilities for damages for financial institutions, this legislation should be amended to provide financial institutions and their employees immunity from civil or criminal liability for any action taken in good faith to protect a senior customer, including discretion to hold a transaction.

The reporting requirements included in HB 2064 as amended also are unmanageable and costly. Reporting requirements for financial institutions should be limited based on circumstances identified by the state Department of Aging. Requirements for producing financial records also should be limited to the financial institution that reports the suspected financial exploitation of the older adult.

Area Agencies on Aging should be authorized to discuss with financial institutions any reports of the financial exploitation of an older adult and the results of their investigations to facilitate decisions to impose or extend a hold, consult with persons reasonably associated with the older adult, or to produce requested financial records. The legislation also should be clarified to include circumstances in which an Area Agency on Aging or law enforcement agency can request a hold be extended or ask that the hold be terminated. Please remember that PACB came to you, the General Assembly, as a partner to address this issue. We are part of the team that is the solution to the problem. Community banks do everything possible to prevent fraud. Please don't punish the people who are trying to prevent harm.

We are fully committed to the process of protecting our customers, particularly our most vulnerable and we will continue to work, every day, to help our customers with their banking needs-the needs of their life.

I [Amy Sgrignoli] am CEO of Belco Community Credit Union. My comments are appended below:

Belco Community Credit Union's Role on Financial Exploitation & Abuse

Preventative

- Member Education
    - Our website contains a safety and security section with important information on how to keep their personal identifiable information (PII) and money safe. This highlights general advice, as well as information on how to spot scams or suspicious requests for information, and how to react to suspicious calls or messages. When in doubt, we tell our members to check with us before doing anything with which they are not comfortable.
    - We collaborate with our Marketing Department on social media strategies that explain to members how to spot scams and how to protect their PII and money.
    - At every opportunity, we counsel our members on how to stay safe. This can be done by any member-facing employee of Belco.
- Employee to Member Support – **Our employees are the #1 tool that we use to keep members protected from financial exploitation/abuse.**
    - Employees are trained regularly to spot activity that is unusual for members and ask questions to the member concerning their transaction history and the purpose of the transactions that they are trying to conduct.
    - We listen for things that don't make sense or seem too good to be true. For example:
        - How did someone win a lottery that they never entered?
        - How could someone be married to someone that they never met face to face?
        - Why does someone serving in the military overseas need help getting home?
        - Why does a person who claims to be an investor have no legitimate business platform, or why would a check be made to a personal name when purchasing a new investment?
    - We observe interactions when elderly/vulnerable members come in with another person.
        - Do we know this other person? Do they come in regularly with our member?
        - Is the other person doing all the talking?
        - Does our member understand what's going on? Are they uncomfortable?
        - Does the transaction seem like something that aligns with their normal activity/lifestyle?
        - Are there any signs of physical or emotional abuse?
    - All member-facing employees have a direct line of support from Fraud Team, who are all highly skilled in spotting and responding to financial exploitation/abuse scenarios. This alliance allows us to address situations in a unified way.
- Artificial Intelligence
    - The Fraud Team utilizes an AI platform that helps us to recognize and interpret account activity that is suspected of financial exploitation/abuse. This gives an additional edge to have supportive discussions with members when an alert is presented to us that may have gone unnoticed without the technology to detect for us.

Reactive

- Memer Intervention
    - Any time we suspect financial exploitation or abuse, the most challenging part is the discussion with the member to reveal to them that they are in a scam. This can sometimes be easy if the member is willing to accept the truth and understands that

Belco employees are trained on these matters, and here to help. More often however, members have been "won over" by the scammer/fraudster. They are convinced that the scam is real, and their judgement is severely clouded by the promise of something positive happening as a result of the transactions that they are conducting. They trust the people taking advantage of them. Even when we can successfully convince someone stuck in that mindset, we often find that they continue to interact with the scammer, finding new creative ways to do things. If a member falls for a scam one time, we consider them vulnerable to fall into that again.

- Recovery
    - We explore all options to help members recover financially if they lose funds. This can include working to stop any payments that have been issued and not yet cleared, working with other institutions to reclaim any remaining funds, or similar.
    - Support is provided to all members as they complete necessary steps, such as getting a device professionally cleaned, placing consumer report alerts, filing a police report, and bringing trusted family or friends into knowledge of the situation.
    - A report to the local Area Agency on Aging will be made if the financial exploitation/abuse victim is at least 60 years old.
- Continued Support
    - We provided members with safety information to notice the red flags of scams, and also share that they can *always* discuss items of concerns with a Belco employee if they ever feel unsure about the authenticity of a financial venture.

Case Examples

Samuel

Samuel is a 75-year-old gentleman who has been convinced that he had won a great sum of money. He was instructed to pay taxes and fees in order to receive his winnings. To do this, Samuel was instructed to purchase and send gift cards to the collectors of the taxes. He was advised to visit numerous gift card sellers because of the dollar limits that sellers impose. Additionally, he took large distributions from his retirement accounts, and with the funds he sent numerous checks (mostly cashiers) over the course of several months for the purpose of paying taxes on the money he won. Our AI fraud monitoring software presented his account to the Fraud Department for review of suspicious transactions. In the first look, the investigator felt uncomfortable with the recent activity on the account, which prompted a deeper look into prior months. Red flags were observed in the transaction history, including out of character ATM withdrawals, as well as checks issued to personal, unrelated names immediately following the deposit of Samuel's retirement distribution deposits. As a next step, we planned a discussion with Sam at his local branch and collaborated with the branch team in advance, shedding light on our concerns.

The Belco team was able to intervene with Samuel at a branch. A supportive discussion was held between the branch staff, a member of the fraud team, and Samuel. We were able to discuss with him what he was going through to obtain these winnings and brought him to the point of realization that he was a victim of a scam.

Samuel unfortunately sent thousands of dollars of his retirement funds to the scammer(s). To support him through the recovery process, we contacted the institution(s) at which the checks he issued had been negotiated at, in an attempt to work with that FI's Fraud Department to have any available funds

returned to Samuel. While this strategy can be successful, in this particular case the funds have been depleted and we were not able to recover anything for him. This is common as fraudsters move stolen funds quickly to evade detection, often making it impossible to recover money for members. We provided Sam with safety information to notice the red flags of scams, and also shared that he can *always* discuss items of concerns with a Belco employee if he ever feels unsure about the authenticity of a financial venture.

Another step we took in Samuel's case was to make a formal report with his local Area on Aging (AOA) for Elder Financial Exploitation. The AOA was unavailable to assist, but we were connected to the public safety office so they could take a preliminary report, which was transferred to local law enforcement and the AOA. While we are not often privy to the outcome of these reports, this is a step that we take often for the protection of elderly members. An agent will perform a check of the individual's wellness including mental, physical, and financial, and are able to support and provide resources whenever necessary.

Linda

Linda is a 73-year-old member who is married and lives with her husband. While on her desktop computer, an alert flashing bulletin appeared on her screen and a voice stating her computer had a virus. The voice stated to not shut down her computer or it would freeze. From her end, it appeared as if the pop-up was coming from Microsoft, and it had a phone number listed for her to contact Microsoft Support. Linda made the call without thinking anything suspicious about it. When she called the number, she spoke to a man who claimed to represent Microsoft who told her that he could fix the issue. Linda gave authority for the man to remote into her computer & view it. He told her he would continue to work on the problem & would call her back the next day to finish.

The following day, Linda was informed that the man downloaded applications to correct the problem and there was cost to fix everything. He used her visa credit card to charge her for the applications he downloaded. Upon doing so, he claimed to have overcharged Linda, so she needed to complete a refund form. The refund of $100.00 was entered incorrect as $10,000.00 and was put into her checking account…or so it appeared that way on her end. He told Linda this money came from Microsoft, and she was responsible for paying it back that same day. With the mindset that she needed to quickly get this money back to Microsoft, she followed the man's next set of instructions to take the overpayment to a Bitcoin ATM. Another person claiming to be from Microsoft provided her with the numbers needed to make the Bitcoin deposit. Linda told him that she didn't feel right about this transaction and told him she was not going to do it, but he assured her the money was NOT hers and belonged to Microsoft. They told her legal action would happen if she did not return it and threatened this a multitude of times.

Another day later, the man from Microsoft called her again to complete computer cleaning. He again claimed to have overcharged her again and would need to do another refund form. This time, Linda thought better of it and checked her bank account and realized that the $10,000 overpayment was in reality an advance transfer from her own credit card into her checking, not a deposit from Microsoft. When she worked with him the prior day, he had manipulated her screen to make it seem that the funds were coming from Microsoft. Linda informed him that she was done giving it and at this point he demanded the password to her computer. He kept threatening to take all her and her husband's money. Linda ended the call and turned her computer off.

Linda immediately called Belco and worked with us to get her debit card cancelled & account secured. She also took steps to have her computer professionally cleaned and serviced. She lost thousands in this scam and felt sad and embarrassed that she had become a victim, and the funds were not able to be recovered.

We provided Linda with safety information to notice the red flags of scams, and also shared that she can *always* discuss items of concerns with a Belco employee if she ever feels unsure about the authenticity of what she is being asked to do.

Donald

Donald is a 77-year-old member who joined Belco in the past two years. After opening his account, he deposited a large check from an investment. Using the funds, several Person-to-Person (P2P) transactions left his account using CashApp and PayPal, and the payments were issued to several different names that had no relation to Donald. Simultaneously, payments using our third-party Bill Payer service provider were being authorized from Donald's account to names that had no relation to Donald.

Our AI fraud monitoring software presented his account to the Fraud Department for review of the P2P transactions. Additionally, the BillPay vendor contacted Belco due to the suspicious activity being initiated in that space, *and* we learned from our call center that an impersonator had called Belco in an attempt to access his account.

On the branch front, Donald visited branches frequently to take large cash withdrawals. The branch employees had good conversations with Donald about the transactions and risks of carrying cash. Donald stated that he was using the funds to make updates to his home and have some improvement completed. Donald also applied for a home equity loan with Belco stating that the funds were intended to pay down debt.

As a next step, we secured Donald's account to stop all activity until we could speak with him and uncover what was the cause of the multiple layers of suspicious activity. The Fraud Team collaborated with the branch network to facilitate a conversation with Donald on his next visit. In that discussion with Donald, he maintained the stance that he was having work done on his home and during this conversation he stated he was replacing his heat pump. He wanted to have cash ready, although he did not have a contractor selected yet or an estimate. We asked him about the other work to his home and if the contractors were going to update his property records with the improvements. He said he wasn't sure, and he would ask them. We could not convince Donald that we were concerned about a scam, and we could not deny him withdrawing his own money. The branch was advised to keep the branch withdraw limit of $2,500. Donald had withdrawn close to $60,000.00 in cash over the course of a few months.

As a next step in Donald's case, we made a formal report with his local Area on Aging (AOA) for Elder Financial Exploitation.

About a month later, Donald visited the branch again for another cash withdrawal and this time made mention of Crypto currency. He was asked to the office for a conversation with a member of the Fraud Team. During the conversation he stated that some of the cash he had withdrawn he deposited to bitcoin ATMs for investments. He shared that he was investing with a woman who told him when to

send the funds once turned to bitcoin to invest. He stated that he did not have access to the bitcoin account to see transactions or earnings; The woman was in control of it. He also stated that he made improvements on his home with some of the cash too. With this new information, we called AOA to update the report.

At this time Donald remains extremely scam vulnerable. His account contains numerous advisory notes available to any staff member who may assist him with transactions.

Nola

Nola is an 80-year-old woman who is unmarried and lives in a lower income demographic. Our first contact with Nola was when she called us with transaction questions. Upon reviewing her transaction history, we noticed a debit card transaction for thousands of dollars at a pharmacy, which immediately appeared that she could be in a scam involving the purchase of gift cards. Nola shared that she did in fact purchase gift cards and sent them to the person who told her to get them. Trying to convince Nola that she engaged in a scam was challenging and she was very confused. We provided Nola with safety information to notice the red flags of scams, and also shared that she can *always* discuss items of concerns with a Belco employee if she ever feels unsure about the authenticity of a financial venture. We added important informational notes to her account that explained that she is scam-vulnerable, and to be extra cautious when interacting with her.

A few days later, Nola brought in a check for thousands of dollars from an out of state maker. The branch observed the information that the Fraud team had attached to her account and attempted to speak to Nola about the check to gather more information, but unfortunately, she was noticeably quiet and not forthcoming. She did nod in agreement with the branch when asked if she was in a possible scam. The check was accepted on hold and was later returned due to fraud.

As a result of the bad check situation and in an attempt to further protect Nola, the Fraud Team disabled Remote Deposit, Zelle, and ATM deposit services to reduce the number of platforms in which a scammer could advise her to conduct transactions.

Another step we took in Nola's case was to make a formal report with her local Area on Aging (AOA) for Elder Financial Exploitation. The Area Agency on Aging has since followed up twice with record requests for Nola.

Nola ended up closing out her account, so the suspicious activity at Belco did stop. However, she may still be involved in scams and conducting her transactions elsewhere as she experienced friction/intervention at Belco.

###

Thank you for allowing us to testify, and please feel free to ask any questions you may have.