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)
October 23, 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; Lauren Greenaway, Fraud Analyst of Belco Community Credit Union and Ed Martel, Chief Operating Officer of Jonestown Bank & Trust Company. 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 was recently refreshed and relaunched earlier this 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.

Need for a Comprehensive Federal Approach to Scam Reduction

Despite their extensive efforts to educate customers to avoid scams, the criminals committing these crimes are extremely sophisticated and resourced with advanced technology that allows them to impersonate legitimate entities. Every financial institution has faced a customer who insists that they know and trust the individual to whom they wish to transfer funds. In the end, it is the customer's money, and most Americans do not want institutions telling them what to do.

Thus, we need a comprehensive national scam and fraud prevention strategy to reduce the ability of criminals to be 'technologically authenticated" by impersonating legitimate businesses such as financial institutions. These efforts need to be coordinated among multiple regulators and connected to law enforcement.

We also need a single, streamlined government reporting process to which to report suspected fraud schemes.

All sectors must see and claim their roles in protecting our critical infrastructure from criminal hijacking.

---

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

State 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;
- 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]

[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

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.

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

---

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.

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 [Ed Martel] am Chief Operating Officer of Jonestown Bank and Trust Company, a $930 million community bank. We have branches in Lebanon, Lancaster and Berks counties. Those branches include Cleona, Cornwall Manor, Ephrata, Grantville, Jonestown, Lebanon, Lititz, Manheim, Newmanstown, Northside Commons (Palmyra), Quentin Road (Lebanon) and Robesonia. We have been in operation since 1873. Since the 19th century we work every day to develop and deliver products that serve our communities' day to day banking needs. Each one of us is involved and committed to our communities. From directors and managers to operations specialists and branch bankers we are actively involved in making a difference in our churches, charities, service clubs, trade organizations and local government. We know our community because we work there and more importantly, we live and raise our families there.

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.

We are constantly on guard against fraud and financial exploitation in an attempt to protect our customers - especially our vulnerable seniors.

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.

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. Both employee and client education and awareness are 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. Those tools range from in person one on one conversations to social media posts, emails and even fraud prevention seminars.

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. Scammers lie to the elderly and claim a bank has been compromised and not to trust any of the bank's personnel. In many cases the elderly are coached to deceive us about what they are doing with their money. It's a recipe for disaster.

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. Banks need the ability to hold and report potentially fraudulent transactions without the fear of violating privacy and discrimination law. Our banks report to the Area Agency on Aging (AAA) but we often 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. When we report to the AAA's we don't know what happens to the reports. We rarely hear anything after we make the report. Often unless someone is in danger of losing their house the AAA's simply don't have the ability or resources to intervene.

The typical experience with any AAA report is that unless a determination is made that the victim is unable to make his or her own financial decisions, there is little that can be done by the Agency. Any follow-up by the Agency is usually only made if the Bank makes contact. Much of this fraud is even outside of the traditional branch banking system, involving FinTechs, credit card processors, crypto and gift card purchases. Some of the stories today discuss wire transfers involving thousands of dollars. But that overlooks the thousands of dollars stolen every day by family members and caregivers.

I'll share with you a few of our bank's experience with the AAA's:

Case #1 – The successor agent (subject) listed in an elderly client's POA documents opened a new account as POA on behalf of the client (victim), claiming the victim was hospitalized and had lost her checkbook. Two weeks later, the victim visited a JBT branch accompanied by her daughter (original agent) and son-in-law and informed Bank staff that the subject refused to turn over any information pertaining to the new checking account, including the checkbook. The victim also stated that she was contacted by the

local police and informed that the subject had attempted to impersonate her and cash a check at another financial institution and had also applied for a title transfer of the victim's automobile. No loss was sustained by the client and a report to Area Agency on Aging was made by the original agent prior to informing the Bank. New accounts were established for the victim.

Case #2 – An elderly client (victim) mentioned to JBT branch staff that his daughter (subject) had been stealing from him. Prior to this report, the subject had contacted Bank staff and informed them that all account discussions should be directed to her, though no POA documentation was on file with the Bank. The subject was informed this would not be possible without the proper documentation. Approximately one month later, a $1,740 check cleared the victim's account, paid to the subject. Attempts were made to contact the victim but were initially unsuccessful and the account was restricted. A report was made by the Bank to the Area Agency on Aging. No follow up was received by the Bank, and after a period of account monitoring after the restriction was lifted the investigation was closed.

Case #3 – An elderly client (victim) had begun making regular cash withdrawals and immediately handing the money to unrelated individuals in the parking lot of a JBT branch. Though the branch would try to dissuade the victim from conducting the withdrawals and would notify the POA each time, the Bank ultimately could not keep the victim from accessing his own funds. A report was also made to the Area Agency on Aging, which concluded that without the victim's willingness to file a police report, there was not much that could be done. The Agency did, however, assist the POA in the process of establishing the POA as Representative Payee. Ultimately, the POA closed the account and opened a new account under the Rep Payee status for the financial wellbeing of the victim.

When we notify law enforcement, many times they tell us not to bother reporting as they don't have the time or resources to follow up. There is a significant need to equip law enforcement with resources and the means to pursue and hold the fraudsters responsible for their actions. Without these resources and significant penalties directed at the criminals perpetuating the scams, we are left to keep addressing the symptoms, not the root cause of the systemic problems facing all citizens of Pennsylvania, including our seniors.

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. In conjunction with increased law enforcement commitment, this would help us stem the tide. 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 could 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 laws.

It must also be recognized that even if a bank stops a transaction many times the fraudster will coach victims to work outside of the banking world. This includes having a senior buy gift cards, money orders, money transfers or making cash withdrawals that can be deposited into a crypto ATM. These funds are lost to the victim immediately and forever.

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 the discretion to hold a transaction. I personally feel the direction should also include direction to law enforcement to take action on reported fraud and be supplied with the resources to do so.

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. If and when practical, existing documentation exists, such as FinCEN required SARs, those documents should be leveraged.

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 am happy to answer any questions you may have.

I [Lauren Greenaway] am Fraud Analyst for Belco Community Credit Union. My comments are appended below:

Belco is a financial cooperative and our mission is to help our members to achieve their financial goals. We take a very proactive role in learning about and helping our members overcome financial challenges and hardships and often become involved when fraud occurs on their accounts. We are here today representing 306 credit unions in Pennsylvania. Pennsylvania credit union asset size averages roughly $238 million with a mean size of about $33 million in assets to provide some scale.

Preventative Measures are taken to mitigate the risk of Elder Abuse and General Fraudulent Financial Crimes:

1. Employee and Member Education:
    a. Website and Home banking include safety and security information on keeping personal identifiable information safe. Things like handling suspicious calls, how to spot a scam, sharing scenarios to heighten awareness of the types of activities that are fraudulent.
    b. Utilize Social Media and Marketing campaigns focused on raising awareness of financial crimes and fraudulent schemes that are happening.
    c. Our employees are the #1 tool that we use to keep members protected from financial exploitation/abuse. We have an area dedicated to fraud – account fraud, loan fraud, any kind of fraud with specialized training in identifying and stopping fraud on member accounts. This area is staffed with two full-time fraud analysts.
    d. Employees are trained regularly to spot activity that is unusual for members and ask questions to the members concerning their transaction history and the purpose of the transactions that they are trying to conduct.

2. The Fraud Team utilizes an AI platform, Verafin, 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.

3. Our Fraud Team is part of South-Central Pennsylvania Financial Security Officers' Association (SCPFSOA) in which members from both law enforcement and financial institutions collaborate on financial fraud.
    a. One of our Fraud Analysts is currently serving as the president of this association.
    b. The group shares hot topics and trends, and importantly fosters collaboration among the network of FIs, Agencies and Law Enforcement. Subject matter experts present on things like ATM Jack-potting, Reg E, Welfare and home healthcare fraud, and education on things like how to contribute the right information to assist cases with Law enforcement.
    c. The group also sponsors several law enforcement officers to attend a training conference each year hosted by the International Association of Financial Crimes Investigators.
4. 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. Belco employees address situations with members by collaborating as a team of specialists.

Reaction is key. We take Action when we detect a suspected fraud instance

1. Member Intervention
    a. Any time we suspect financial exploitation or abuse, the most challenging part is the discussion with the members 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 because of the transactions that they are conducting. They trust the people who are 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.

b. We add important informational notes to accounts to explain when members are scam-vulnerable, for front line and phone employees to be extra cautious when transacting business on these accounts.

2. Recovery
    a. Pursue 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.
    b. 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.
    c. A report to the local Area Agency on Aging will be made if the financial exploitation/abuse victim is at least 60 years old. Formal reporting is a common practice when the signs of fraud exist.
    d. While we don't often know outcomes we continue to actively engage in reporting.
    e. Provide Ongoing Support after an incident: We provided members with safety information to notice the red flags of scams and 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.

Examples have been detailed and entered formally as part of testimony today:

Common themes from our examples are:

1. Scammers are targeting unsuspecting vulnerable seniors who are likely to be technically challenged or unaware.
2. Fraudsters are persistent with Multiple contacts are made to build rapport and what seems like relationships.
3. Many times, fraud is an overly complicated transaction that leads to confusion and vulnerability.
4. At times there is a reluctance by the victim to admit their mistake – and friction with the intervention by Belco's fraud team.
    a. Overwhelmingly embarrassed
    b. Reluctant and Emotional about their mistake
    c. In some cases, loyalty to the Fraudster is due to promises of home improvements or things like monetary winnings.
    d. Threats of fictitious legal action leave seniors scared.
5. In some cases, the fraud continues, Victims may still be involved in scams and conducting their transactions elsewhere – because they still believe the fraudsters and are too emotionally involved in the scheme.

6. Fraudsters are preying on our vulnerable population; using fear; using technology to confuse and defraud their victims.

These are a *few examples – there are more; they keep coming and with the addition of AI, the schemes become more frequent and more elaborate; harder to slow down; our resources are outpaced by the volume of attempts we are seeing.*

Despite all our efforts – the senior population remains susceptible to these crimes. These are financial crimes; fraudsters are literally stealing money from PA citizens. *Much like the Central Pa Fraud group does, We need to work collectively to create tools to fight this crime.*

Our team is taking a collaborative approach both internally and externally - internally with our front-line teams and externally with law enforcement and area agencies on aging.

We see this as an opportunity to partner with the legislature. Take actions that create workable solutions to the problems. Protect our seniors and our financial systems and reduce broader financial crimes risks.

As written, the legislation needs work, we are concerned about discriminatory practices against seniors.

- If we block all transactions when we need to only block what makes sense, seniors are inconvenienced and singled out.
- Penalties to the financial institution will force us to hold more, exacerbating the situation. 30-40K fines is material. This reduces revenue to staff our credit union's fraud team, take away the ability to keep current technologies and training in front of our team – especially at when margins are compressed – cost of doing business is at an all-time high, delinquency is rising and pressure to remain sustainable exists.
- Blocking access to seniors may in fact push them to even higher risk means or methods of moving money.
- Our Agencies will become backlogged and may not be equipped to handle the volumes,

Together, the legislature, area agencies and financial institutions can do good things; we are encouraged by the invitation here today and hope that together we can make the final legislation balanced to work for our community partners and to project our seniors.

Example Details:

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.

- 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 account to the scammers. Our team worked with Samuel to recover the stolen funds but unfortunately were not successful. Formal reporting with the Area of Aging for Elder Financial Exploitation. AOA performs a check of the individual's wellness including mental, physical, and financial, and can support and provide resources whenever necessary to review suspicious transactions. Samuel has sent thousands of dollars of his retirement.

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. 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. She subsequently 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 scam involved charges for these services, overcharging, refunding to credit cards and deposits to checking accounts leaving Linda confused by what was happening in her account and she ended up making a bit coin ATM payment of 10K to what she thought was Microsoft. The following day a similar request came through which then made her suspicious enough to call Belco and request assistance.
- 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.

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 to attempt to access his account.
- 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.
- 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.

###

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