Testimony of the Office of Attorney General
on behalf of Attorney General Michelle A. Henry
Before the Senate Committees on Aging & Youth and Banking & Insurance
Joint Public Hearing on Protecting Seniors from Financial Exploitation

September 18, 2024

Delivered by John Abel, Chief Deputy Attorney General and
Nicholas Smyth, Assistant Chief Deputy Attorney General

Good Morning, Chair DeSanto, Chair Street, Chair Ward, Chair Collett, Vice Chair Gebhardt, and members of the Committees. My name is John Abel, and I am the Chief Deputy Attorney General and Director of the Bureau of Consumer Protection.

My name is Nicholas Smyth, and I am the Assistant Chief Deputy Attorney General. I have been leading the Office of Attorney General (OAG)'s work on consumer financial issues since 2017, and before that I had various roles in the Federal government and private sector. Governor Shapiro hired me in 2017 to expand OAG's work in the banking and finance space. Under his leadership, we obtained massive settlements with the biggest financial institutions, including Wells Fargo, Citibank, Navient, and Equifax. Since July 2017, OAG's finance cases have led to more than $373 million in direct relief for Pennsylvania, directly impacting nearly 500,000 Pennsylvanians. Much of this money went to the Treasury, and the bulk of it went directly to the Pennsylvanians who were harmed by these big corporations.

Thank you for holding this hearing and for inviting the Office of Attorney General to testify on the urgent issue of protecting seniors from financial exploitation. Over the past few weeks, we have been working with your staff, and we appreciate that you and they have been working diligently on these issues for a long time. We also appreciate all the work that the Department of Aging, including Secretary Kavulich, and the Governor's Office have put into this legislation.

HB 2064 is an imperfect but good bill that is much better than the status quo. And it passed the House with overwhelming bipartisan support.

We appreciate that many banks are eager to do more to protect their customers, and they have been pushing for a report and hold law for several years now. HB 2064 would give the banks the tools they want and need - including immunity - to stop many of the fraudulent transactions.

We are eager to work with the administration, the General Assembly, and stakeholders to get HB 2064 passed into law. HB 2064 and the larger Older Adults Protective Services Act rewrite are urgently needed. Our testimony has three parts: first, we provide basic background on the

cyberfraud crisis, second, we share some real-world examples, and third, we explain how HB 2064 would enable the banks to stop the fraud.

I. Criminal Gangs are Stealing Massive Amounts from Pennsylvanians' Life Savings.

Nationwide, the Federal Trade Commission (FTC) estimates that criminals stole between $21 billion and $137 billion in 2022. Based on the FTC's data, OAG estimates that criminals stole between $800 million and $5 billion from Pennsylvanians in 2022. [1] (These estimates vary because it is hard to know the magnitude of underreporting of fraud.)

Again using the FTC estimate, OAG estimates that criminals stole from Pennsylvanians over 60 between **$260 million to $2.1 billion**. These numbers are enormous. To give you the sense of the size:

- Fraud losses by seniors in PA are at least as high as what PA taxpayers will provide in support for Penn State University this year ($276M in 2024-25)
- Fraud losses by seniors could be as high as $2.1 billion, which is more than what PA taxpayers spent on all state-related universities and the state system of higher education, including grants to students ($1.822B) plus the Dept of Military & Veterans Affairs ($227M) (total of $2.05B).

Our estimates are in line with private sector estimates. Using PA data, Comparitech estimates **$1.63 billion** stolen from **28,113 PA seniors** in 2022/23 – a 26% annual increase in number of victims. This is an average of $58,000 per crime victim.

President Eisenhower once said, "I have two kinds of problems: the urgent and the important. The urgent are not important, and the important are never urgent." This issue is an exception. Because of the growth in dollars lost and victims harmed each year, cyber fraud losses are both important and urgent.

Instead of Pennsylvania's retirees being able to spend their hard-earned savings here in the Commonwealth, supporting our small businesses, and paying taxes here, overseas gangs are stealing people's entire life savings. These gangs are taking billions of dollars out of Pennsylvania, out of the US, and reinvesting it in their fraud operations.

The criminal gangs are perpetrating the fraud using human trafficking victims in places such as Cambodia and Myanmar, often masterminded out of China. They have set up office parks full of people who've been lured there with the promise of high paying customer service jobs. Once they show up, they're told that they can't leave, their passports are taken, and they're forced to run these scams, and beaten or tortured if they don't. Every month, the criminal gangs reinvest

[1] **$800 million** is more than the 2024-25 taxpayer support for state-related universities (Pitt, PSU, Temple, Lincoln, & Stevens). **$5.3 billion** is more than PA has budgeted on all higher education ($1.822B), Military & Veterans Affairs ($227M), and the Dept of Corrections ($3.153B).

their profits and expand their fraud empires. The longer we wait to act, the harder it will be to stem the tide of fraud losses.

The theft of billions of dollars from Pennsylvanians' bank accounts affects all of us. It reduces the money available for Pennsylvanians to pay for higher education, buy a home, start a business, get married, have kids, or retire. And it reduces the money the banks have on deposit, which means they have *billions less* to lend to businesses and consumers each year.

II. OAG Devotes Significant Resources to Helping Crime Victims. Under Current Law, Most Victims are Not Getting Their Money Back.

Our office has prioritized cyber fraud response since Josh Shapiro became Attorney General in 2017. Under his leadership, we set up a rapid response Scam Team that was the first in the nation. Attorney General Michelle Henry has continued to bolster the team, which now has five dedicated employees and special procedures. When a scam complaint comes in, we immediately contact all the financial institutions involved to try to reverse the transactions. Sometimes we get lucky and the money is still there. But the sad fact is that, today, most of the money stolen through financial fraud is never returned. Even with our hard and fast work, last year we managed to recover only 2.5% of the dollars that Pennsylvanians reported losing.

Of the fraud losses reported to our office last year, nearly 60% of the total dollars started as a wire transfer from the victim's bank account. And while nobody in the banking industry wants this to happen, it's still happening.

If the banks were better incentivized to stop the fraud as they are with card payments under current law, they would quickly develop a system of identifying and blocking risky transactions. And often it wouldn't be very difficult to identify the signs of fraud. The criminals typically ask their victims to wire a vast amount of money in a short time, frequently to LLCs that are across the country. And most victims have rarely if ever sent a wire before.

At some banks, particularly smaller banks, the crime is sometimes headed off by a conscientious teller or customer service agent. But the story is different at certain very large banks. These banks allow wire transfers to be sent using their websites or apps alone, even for hundreds of thousands of dollars. And even if a customer goes into a branch or calls to request a wire, the bank is not asking enough questions about the purpose of the wire.

A. Scott Zeiders of Harrisburg

Scott Zeiders is a retired forklift driver who has lived in Harrisburg his whole life. Criminals stole $12,000 from Scott, 69, by using stolen credentials to hack his mobile phone account in October 2023. This enabled the criminals to intercept a one-time SMS verification code from his bank, Wells Fargo. The criminals also used the stolen login credentials to initiate a wire transfer from the bank, which did not call him to verify the wire, even though he had voice verification on his account. Scott told us, "I can't believe they would transfer $12,000 without verifying me.

But to talk to me they make me do voice verification." If Wells Fargo had called to ask Scott why he was wiring the funds or required him to come into a local branch first, the fraud would have been prevented. It is only in the past few years that banks have allowed wire transfer requests without any human interaction.

Scott ultimately got his money back after Seth at ABC27 News covered his story and started asking Wells Fargo questions. He believes Wells would not have reimbursed him but for the media coverage.

B. Judith from Reading

Judith, 70, is a retired clerk in the Reading area. She serves on her local VFW Auxiliary. She participates in line dancing and loves to read.

In April 2022, criminals attacked her with a tech support fraud. They froze her computer a put a big alert across the screen. Judith told us it made a loud siren, like an air horn. Terrified, she called the phone number in the pop-up message. The criminals told her that a $30 refund would be issued for improper installation of a program, and they instructed her to provide remote access so that they could "walk her through" the refund process. The criminals then made it appear as though *Judith* had mistakenly requested a $30,000 refund. The criminals said it was an error and that they would need her to fix it.

Judith felt horrible and wanted to make it right. At the criminals' direction, Judith went to her bank and wired $29,500 to their account. Two days later, she realized this was a scam and contacted her credit union to place a freeze on the account. The initial wire return request was denied by Wells Faro (the bank the criminals had her send the money to). But Judith reported the crime to the Lower Heidelberg Twp. police department, where an incredibly persistent detective, Jordan Smith, works. Det. Smith diligently followed the money and ultimately recovered most of it from a bank in Virginia. This is a very unusual outcome. Most of the time, the local police do not have the resources to quickly contact multiple financial institutions. Typically the money is already gone, overseas, and the accounts are closed. Judith was fortunate to have Det. Smith on her case.

C. Bill Hoffman of Lebanon

Bill, 62, grew up on a dairy farm and is a lifelong resident of Lebanon. In February 2023, criminals began scamming him through a fake online cryptocurrency investment platform called Bitzoom. Through this platform, the criminal gangs provided a very believable investment program that seemed to be a legitimate site. Before investing, Bill looked up the company and found that it was registered and in good standing with the Colorado Secretary of State. He also searched for the domain name and discovered that it was hosted by Amazon Web Services, which further reinforced his belief that it was a legitimate cryto platform.

At the outset, Bill's bank – a national bank with over $10 billion in assets headquartered in PA – approved his requests to wire huge amounts of money to obscure LLCs[2] in California even though he told them the wires were for investments in Bitcoin – an obvious red flag.

Across the span of approximately four (4) months, the criminals convinced Bill to send a total of $1.5 million, which includes not only his life savings, but also money borrowed through a home equity loan against his home. Bill's bank could have easily prevented the whole fraud if it had just recognized the obvious red flags on the initial wire transfer – and it could have still saved him over $1 million in losses if it had recognized the red flags on the subsequent wire transfers in the next five weeks.

Bill explained, "Before I ran into this, I didn't have a mortgage or home equity loan. I had some money in a 401k. Now I have lots of debt. From month to month we continue to make things work."

D. Ronald Funk of Lebanon

Criminals stole $29,900 in January 2023 from Ronald Funk, 62, of Lebanon by impersonating the seller of a motor home on RVT.com, a legitimate classifieds website. The criminals provided a real VIN and Carfax, but they were not the true owners of the motor home. After doing his due diligence on the motor home and the "seller," Funk signed a purchase agreement and wired the purchase price ($29,900) to the criminals' account.

Funk realized within two business days that it was fraud and promptly contacted his bank, Wells Fargo, to inform them. The bank took two weeks to respond. On February 9, 2023, Wells Fargo, which Funk has been banking with his "whole life," declined to reimburse him for the fraudulent transfer "due to this being an authorized transaction with no error." Funk estimates he spent a thousand hours trying to track down the criminals. Wells Fargo told Funk that they knew where the money went but would only release this information to law enforcement. The financial institution utilized by the criminals, Chase Bank, refused to release information to Funk about the criminals' account, stating only that it was a business account "in good standing." Funk believes that "Banks should give up the information when a crime has been committed like this."

When Funk contacted RVT.com to report the fraud and ask for the information on the individual(s) who listed the motor home, RVT told him that they could not release that information. A week later, RVT claimed that the record of the individual(s) responsible for the listing had been deleted. Funk stated: "I love camping. I was looking to buy a perfect motor home for me and my family to camp in. I never was able to buy a new motor home. I still think about it. How could somebody do what they did, and then somebody not be willing to help you find out who did it to you? I think there have to be more protections."

[2] $90,000 on 3/10/23 to KQQ Kitchen Appliance Wholesale LLC, $105,975 on 3/17/23 to Aurorral Trade Inc, $74,999 on 4/3/23 to Yi Shun Dan Trading Co, and $200,000 4/18/23 to Yi Shun Dan Trading Co.

These are just four examples from the 26,000 Pennsylvania seniors whom criminals steal money from each year. We appreciate them courageously allowing us to tell their stories publicly in order to help get this legislation passed. They and other victims want to help save others from experiencing the same horrible fate.

III. HB 2064 Would Give Banks the Tools They Need to Stop the Criminals in Their Tracks.

Like other states' laws, HB 2064 would require financial institutions to report any suspected elder financial exploitation. Reporting is important, but it's not the most essential piece. In our view, the most important thing HB 2064 does is enable and encourage financial institutions to hold a transaction if they suspect elder financial exploitation. And it gives the institutions *immunity* from civil suits for placing a hold on a transaction.

The reimbursement provision ensures the bank will place holds when it suspects elder financial exploitation.

Giving banks immunity for placing a hold is important, but immunity alone will not solve the problem. Banks already have authority to place holds when they suspect money laundering – which much of this fraud is – and they rarely do. Banks need skin in the game.

For decades, the banks have done a very good job at preventing credit card and debit card fraud because they have skin in the game and individual account holders are protected against fraud losses. We believe the banks will become just as good at preventing fraudulent wire transfers and other payments if HB 2064 is enacted.

Just as banks are not *required* to reject a credit card purchase if they suspect fraud, HB 2064 does not *require* a bank to hold a wire transfer when it knows or suspects financial exploitation. Instead, banks are incentivized to stop credit card fraud because they are liable to reimburse customers for losses.

HB 2064's liability provision (606(b)) would better incentivize financial institutions to place holds when large amounts of money are at stake. It appropriately allocates the risk between the consumer and the bank, based on who can control or prevent the loss.

Under limited circumstances, Sec. 606 allows the consumer to seek reimbursement from the financial institution. Sec. 606 is narrowly tailored to provide necessary incentives without creating pressure on the bank to hold every little transition. Unlike in the credit card space, there are significant hurdles that a fraud loss must satisfy before it becomes reimbursable.

Under 606(b), the financial institution would be liable for **an older adult's financial losses** due to **financial exploitation** only if all four hurdles are met:

1) **Designated representative** (a specially trained person at the bank) knew or had reasonable cause to believe that the older adult was subject to past, current or attempted financial exploitation;

2) Despite such knowledge or reasonable cause to believe, the **designated representative** failed to hold a proposed transaction;

3) Within **60 days after such failure to hold**, at least **$10,000 in the aggregate** was stolen from the older adult's account over a **period of 31 days or less; AND**

4) **Within 180 days** of the last transfer, the financial institution was **notified in writing**, under **penalty of perjury,** that the transfer was a result of financial exploitation

Together, these hurdles ensure that in egregious cases older Pennsylvanians who lose their entire life savings can get their money back. But it will not protect the older Pennsylvanian in all circumstances. And for Pennsylvanians who have less than $10,000 to lose, HB 2064 leaves the decision to reimburse entirely to the bank.

<u>The penalty provision only applies to government actions, and penalties are not automatic.</u>

Today other witnesses may raise concerns with the penalty provision in Sec. 606(a). OAG is open to discussing a tiered penalty that starts lower than $10,000. But it is also worth noting two things that significantly limit the application of the penalties. First, only OAG or the Department of Aging can enforce the penalty provision – not a private plaintiff. Second, $10,000 is just the *maximum* penalty that a Court may order, so even when OAG or Aging does seek penalties, a Judge will ultimately decide the penalty amount based on the nature of the violation. In other words, the penalty is not automatic and the Judge in deciding the amount would have the opportunity to consider the totality of the facts.

***

In sum, the cybercrime crisis is devastating Pennsylvania. This legislation will cause banks to be more cautious in approving wire transfers, which will drive down fraud. Many consumers who lose money will not be able to satisfy the high bar of Sec. 606, so they will not get their money back. But some will – and the risk of that will ensure the biggest banks do a better job stopping fraud.

Thank you for conducting this hearing, and we would be happy to answer any questions.