Stopping Advance-Payment Scams in Advance

Tyler Moore

School of Cyber Studies, College of Engineering & Computer Science,
The University of Tulsa, OK, USA tyler-moore@utulsa.edu

Abstract. Advance-payment scams affect thousands of people each year, causing billions in losses. Victims are duped into sending large payments to scammers offering a variety of ruses. This paper proposes a simple defense against such attacks: account holders can adopt safeguards *in advance* that limit the size of allowed transfers, introduce delays, and notify trusted contacts.

1 Introduction

In a common form of cybercrime, individual victims are duped into sending money to scammers. The details of the ruse can vary, from classic advanced-fee frauds where victims are promised huge sums of money in exchange for first sending a modest fee, to fake tech support operators promising to fix a non-existent computer problem for a fee [6], to impersonating government agents who request funds to aid in crime prevention or avoid stiff penalties. In 2023, 164,910 such *advance-payment scams* totaling $6.6 Billion were reported to the US FBI Internet Crime Complaint Center [14].

These scams create a sense of urgency in victims to act quickly without consulting others, adhering to the "need and greed" and "time" scam principles identified by Stajano and Wilson [8]. While many victims are elderly, victims come from all ages and educational and professional backgrounds. To defend against these scams, experts train consumers to recognize the telltale signs. They are also reminded not to send money to strangers. Notably, the onus is placed on the individual to take the right steps when encountering a scam. Unsurprisingly, these defenses often fail. Scammers can be quite convincing, preying on human fallibility and cognitive biases to dupe victims.

This paper discusses an alternative approach to combating advanced-fee frauds. The idea is simple: enable people to place restrictions on large outgoing financial transfers *in advance*, before any scam takes place. The remainder of the paper will discuss details about the options for such restrictions. To be effective, the restrictions should (1) introduce a delay to large transactions, (2) notify one or more named associates of the pending transaction, and (3) be impossible for the account holder to circumvent. Putting these restrictions in place in advance creates a credible deterrent to scammers, prompting them to move onto other targets. If enough people and institutions adopt these countermeasures, entire classes of cybercrimes could be eradicated.

29th International Workshop on Security Protocols (SPW), Trinity College, University of Cambridge, March 26–27, 2025.

2 Advance-Payment Scams Overview

The retired lawyer Barry Heitin lost $740,000 of his retirement savings to scammers [2], who tricked him into believing that he was aiding an important law-enforcement investigation. Several details of his experience illustrate what defenses are needed to protect people like him in future. The scam started when he was directed to call a fake phone number claiming to be his investment account's fraud department. A scammer posing as an IRS agent offered to safeguard his money by transferring it to a "federally controlled" account. He complied, sending $113,000 from his checking and savings accounts in a series of transfers. He was then convinced to move funds from his retirement accounts, which held more than $830,000. When his financial adviser expressed doubt over the legitimacy of the withdrawal requests, the scammers directed Heitin to roll over his funds to a different brokerage who would prove less scrupulous. In other cases, such as his bank and gold dealer, individuals expressed concern to the victim that the transactions could be fraudulent. But they ultimately did not block the requests.

New York Magazine financial-advice columnist Charlotte Cowles recounted how she was quickly scammed out of $50,000 [3]. She received a phone call purportedly from Amazon claiming to have identified fraudulent purchases on her account. The agent transferred her to someone claiming to be from the FTC, who explained that her identity had been stolen and used to make many large purchases. He offered to help protect the money in her bank account, which ultimately led her to withdraw $50,000 in cash from her bank and deliver it in a shoebox to an unmarked vehicle outside her home. The scammer managed to get her to act fast: fewer than 12 hours passed between the fake call from Amazon and the money being delivered to the scammer. Moreover, the scammer also successfully discouraged Cowles from telling anyone, including her husband.

We can draw several lessons from these examples. First, neither victim sought out the scammer. Instead, they responded to a carefully crafted impersonation initiated by the criminal. Second, the scammers guided victims to quickly transfer large sums in an irrevocable manner. Third, victims were isolated from others who might have talked them out of taking action. Fourth, financial institutions did not put up much of a fight against the scams. Responses ranged from individuals expressing concern to complying without raising any questions.

These payment scams are not isolated examples. The Internet Crime Complaint Center (IC3) publishes statistics on self-reported cybercrimes [12,13,14]. They report on 26 distinct categories of cybercrime. Of these, 15 involve direct financial losses. Table 1 reports the average annual losses associated with these categories for 2021–2023. We further split them into two types, payment scams involving individuals and others. We focus on the first type as these scams are most amenable to the proposed defenses. We observe that the payment scams average 150,000 reports annually, with self-reported losses exceeding $5 billion. It is also worth noting the mean loss for each category. Most exceed $10,000, with an overall average exceeding $30,000.

While we expect the loss distribution to be skewed, such data is not reported by IC3. Simpson and Moore analyzed BEC losses reported to IC3 at the record

Advance-Payment Scams: Potential to Stop in Advance

Cybercrime Category	#	Annual Loss	Mean Loss
Investment	30,220	$3,112.7M	$98,263
Confidence Fraud/Romance	20,381	$781.5M	$38,215
Real Estate	10,942	$297.5M	$26,454
Tech Support	31,334	$692.9M	$21,316
Lottery/Sweepstakes/Inheritance	5,270	$83.1M	$16,457
Advanced Fee	10,114	$112.5M	$11,642
Extortion	42,333	$63.2M	$1,490
All Payment Frauds	150,594	$5,143.4M	$34,154

Other Frauds: Unlikely to Stop in Advance

Cybercrime Category	#	Annual Loss	Mean Loss
Business Email Compromise (BEC)	21,092	$2,695.0M	$127,606
Ransomware	2,980	47.7M	$16,237
Credit Card/Check Fraud	17,818	203.6M	$11,492
Identity Theft	33,110	197.9M	$6,182
Non-Payment/Non-Delivery	61,560	309.6M	$5,224
Overpayment	5,478	35.9M	$4,885
Employment	15,214	56.6M	$3,712
Phishing/Spoofing	320,836	101.7M	$310
All Other Frauds	478,087	$3,648.0M	$7,630

Table 1. Average annual cybercrime losses reported to FBI IC3 (2021–2023). Top rows indicate payment scams that could be stopped if precautions adopted in advance.

level [7], finding that some victims lost much more than others. Nonetheless, the mean provides a decent approximation of what individual losses could be.

3 Protocol Design

To counter advance-payment scams, financial institutions could add the following requirements. First, customers are asked to provide the name and contact details of at least one *trusted contact* who should be notified in the event of a large financial payment request. A stronger defense would be to require approval from the trusted contact before approving large payments.

Second, customers are asked to confirm the transfer amount that would trigger an intervention. A default threshold could be set, such as $10,000 or $15,000, to be consistent with average losses. Since spending habits vary widely, permitting adjustments would help minimize false alerts.

Third, a time delay should be established for payment requests exceeding the threshold. 24 hours could be sufficient for some scams, but it could be extended to as much as 30 days unless or until a trusted contact verifies the legitimacy of the transaction.

For the countermeasures to be effective, they must be in place before a scam is initiated. Hence, it makes sense to select these choices when an account is opened. For existing customers, a periodic review and reminder could work. The process could operate similarly to naming beneficiaries.

Although not foolproof, these simple protections could help counter many advance-payment frauds. Speed and isolation are key to the success of many such scams. These precautions slow the transaction process down and raise awareness to other individuals who may be able to intervene on behalf of victims.

Possible Objections and Protocol Adjustments Given its simplicity and potential effectiveness, why is this approach not already in place? Incentives provide a partial explanation. Account holders lose their own money when scammed, and banks are not liable for reimbursing their customers. Yet financial institutions would bear the cost of implementing the safeguards. Their priority is to enable faster payments with less friction, the opposite of what is proposed here. They would also have to deal with the cost of interacting with customers who want payments to go through.

Privacy presents another concern. Having the means to send large payments reveals information about the account holder's wealth. This information could be abused if the named contact is not trustworthy. Moreover, prior research has already established that financial technologies are poorly equipped to deal with situations involving intimate-partner violence [1]. This would undoubtedly be true for the proposed mechanism as well.

Moreover, not everyone has a trusted contact that they would be comfortable with sharing such details. For joint accounts, establishing one trusted contact could be automatic. In other cases, it may be harder to establish.

Given the importance of the trusted contact and its potential for abuse, one promising option would be for the trusted contact to be provided as a service by a company with appropriate expertise. This might work in a fashion directly analogous to financial trusts, which can name individuals or institutions as trustees. Trust companies routinely provide the trustee service when no suitable individual is available, bringing expertise and objectivity to decision-making. In a similar vein, service providers could be named as trusted contacts. They would in turn be responsible for evaluating suspicious transactions and postponing or blocking them when suspected of being scams. In addition to mitigating risks to privacy and abuse by people close to account holders, such a model also brings the benefit of outsourcing the expertise required to reliably assess when a scam is taking place.

It is also possible that legal barriers may prevent implementing these changes. We observe that in the US, investment firms have the option to establish a trusted contact who can receive information about an account [5]. This could include notifications about suspicious transactions, though the onus is on the institution to notify and the contact has no authority to slow or stop transactions. A different regulation permits institutions to temporarily freeze suspected transactions for customers who are over 65 or are mentally disabled [4]. Participation is voluntary.

There is an inherent trade-off between integrity and availability. Being more aggressive in blocking fraud, i.e., by setting lower financial thresholds, longer delays and requiring trusted contacts to authorize transactions, necessarily increases the chances legitimate transactions are slowed down or blocked entirely.

Yet permitting account holders to change these configurations once a potential scam has been initiated would defeat the purpose of instituting them in the first place. Hence, taking care to set configurations that minimize false positives is important. Additionally, one could permit changes to take place any time a large transaction is not pending, so long as there is a delay in the changes taking effect.

Another question is whether these safeguards should be voluntary or mandatory to adopt. Requiring all accounts to follow the additional rules would certainly put the largest dent in the success of scams, but it would also invite the strongest resistance from the financial industry (and some consumers). A voluntary approach seems more palatable as a first step.

How would attackers react? In the first instance, they may move onto victims who have not enrolled in the additional protections. If enough accounts are protected in this way, attackers may take steps to circumvent the precautions, like initiating many payments below the threshold. This would still count as a partial success for the defense, as the pace of attack is slowed and the likelihood of being flagged for fraud will increase. They may also wait out any time delays. Again, this would be a partial success, because the delay will give more time for victims to recognize what is happening and exit the scam.

Comparison to Alternative Defenses Some banks may already offer similar protections, particularly to higher-value clients. We have not observed any public examples available to all clients. Such one-off arrangements, while valuable to those enrolled, have not scaled.

One common defense is for institutions that are being impersonated to remind people that they would not do the things scammers are. See for example: “The FTC will never threaten you, say you must transfer your money to “protect it,” or tell you to withdraw cash or buy gold and give it to someone. That’s a scam. Report it” [15].

These warnings tend not to help much. Victims who are already in thrall to scammers usually ignore this advice, or readily accept the excuse provided by the scammer to disregard it (as the victims discussed in Section 2 did). Of course, in most cases the victims do not even see this advice until after the scam is completed. The advantage of the proposed method is that people can adopt the protections before the scam is initiated, which makes it impervious to persuasion by scammers later on.

Finally, we do note that ex post regulation has been tried. UK regulators have recently made payment providers liable for authorized push payment (APP) fraud [9]. It will be interesting to see how both banks and fraudsters react to these rules. Banks might become more aggressive in policing fraud and lowering transaction limits, while fraudsters could move to payment methods that are not as heavily monitored. The US Department of Justice has reached settlements with money-services businesses to compensate victims for their role in facilitating such frauds. Western Union forfeited $586 million [10] while Moneygram agreed to pay $115 million to 40,000 victims [11]. Such punitive actions might theoretically incentivize better behavior. In practice, though, advanced-payment scams continue to leverage their platforms.

4 Conclusion

Advance-payment scams present a significant and growing threat. People's lives are routinely ruined by cybercriminals who can extract the life savings of victims.

We presented a simple countermeasure for consideration. Before any scam attempt takes place, account holders can arrange to delay large payments and require notification or approval by trusted contacts that are named in advance. While such defenses are far from foolproof, such additional friction may often be enough to slow transactions and prevent scams from ultimately succeeding.

As discussed, adopting these techniques would introduce costs. Threats to privacy and coercion by people known to account holders are real risks. Many legitimate transactions will be slowed, introducing a small but nonetheless significant cost to normal payments. Ultimately, a cost-benefit analysis comparing these downsides to the potential benefits should be undertaken. Much of the data needed to undertake such an effort is held by private institutions. The available public evidence suggests that countermeasures would likely bring benefits that far outweigh the costs introduced.

References

1. Bellini, R., Lee, K., Brown, M.A., Shaffer, J., Bhalerao, R., Ristenpart, T.: The Digital-Safety risks of financial technologies for survivors of intimate partner violence. In: 32nd USENIX Security Symposium (USENIX Security 23). pp. 87–104. USENIX Association, Anaheim, CA (Aug 2023), https://www.usenix.org/conference/usenixsecurity23/presentation/bellini
2. Bernard, T.S.: How one man lost $740,000 to scammers targeting his retirement savings. New York Times (July 2024), https://www.nytimes.com/2024/07/29/business/retirement-savings-scams.html
3. Cowles, C.: The day I put $50,000 in a shoe box and handed it to a stranger. New York: The Cut (February 2024), https://www.thecut.com/article/amazon-scam-call-ftc-arrest-warrants.html#/
4. FINRA: Rule no. 2165: Financial exploitation of specified adults (2025), https://www.finra.org/rules-guidance/rulebooks/finra-rules/2165
5. FINRA: Rule no. 4512: Customer account information (2025), https://www.finra.org/rules-guidance/rulebooks/finra-rules/4512
6. Miramirkhani, N., Starov, O., Nikiforakis, N.: Dial one for scam: A large-scale analysis of technical support scams. In: Network and Distributed Systems Security (NDSS) Symposium (2016)
7. Simpson, G., Moore, T.: Empirical analysis of losses from business-email compromise. In: APWG Symposium on Electronic Crime Research (eCrime). IEEE (2020), https://tylermoore.utulsa.edu/ecrime20bec.pdf
8. Stajano, F., Wilson, P.: Understanding scam victims: seven principles for systems security. Commun. ACM **54**(3), 70–75 (Mar 2011). https://doi.org/10.1145/1897852.1897872
9. Sullivan, J.: APP fraud: The UK's mandatory reimbursement requirement. Thomson Reuters (2024), https://www.thomsonreuters.com/en-us/posts/investigation-fraud-and-risk/app-fraud-uk/

10. U.S. Department of Justice: Western Union admits anti-money laundering and consumer fraud violations, forfeits $586 million in settlement with Justice Department and Federal Trade Commission (2017), https://www.justice.gov/opa/pr/western-union-admits-anti-money-laundering-and-consumer-fraud-violations-forfeits-586-million
11. U.S. Department of Justice: Nearly 40,000 victims receive over $115m in compensation for fraud schemes processed by MoneyGram (2023), https://www.justice.gov/opa/pr/nearly-40000-victims-receive-over-115m-compensation-fraud-schemes-processed-moneygram
12. U.S. Federal Bureau of Investigation: Internet crime report (2021), https://www.ic3.gov/AnnualReport/Reports/2021_IC3Report.pdf
13. U.S. Federal Bureau of Investigation: Internet crime report (2022), https://www.ic3.gov/AnnualReport/Reports/2022_IC3Report.pdf
14. U.S. Federal Bureau of Investigation: Internet crime report (2023), https://www.ic3.gov/AnnualReport/Reports/2023_IC3Report.pdf
15. U.S. Federal Trade Commission: How to avoid imposter scams (2024), https://consumer.ftc.gov/features/how-avoid-imposter-scams

Stopping Advance-Payment Scams in Advance (Transcript of Discussion)

Tyler Moore

The University of Tulsa

Session 1 Talk 1

Susan Landau: I actually found myself in a situation where I had to set up a large account and move money at short notice. We were lucky that we were able to move things relatively quickly, although not as quickly as we would have liked. My brother was going to be in charge, which was fine. My sister-in-law was traveling in Patagonia, so it was lucky it wasn't using my sister-in-law, because of the trust. You don't have enough of a backup in there if the trusted party is available. One or two are available, and not everyone is available 24/7. Sure, it says at least one, but people will choose one and then get stuck. Additionally, I'd like to have data before trying to institute something like that, to understand the extent of the problem and what the banks are doing now.

Reply: I agree 100% that this is, at this stage, very far from usable. But I would love to hear ideas and suggestions for what can be done.

Kyle Beadle: Have you considered situations of domestic abuse? I think this protocol could facilitate harm, particularly because even if it's set up in advance, an abuser might force their victim to name them as their trusted contact.

Reply: What would be the harm from them being the trusted contact? How much power does that give them?

Kyle Beadle: It essentially prevents escape. The victim wouldn't be able to withdraw enough funds to escape their abuser.

Kieron Ivy Turk: This is a very related point, but from another perspective: if you have a domestic abuser who is the trusted contact for a victim or survivor of abuse, this could potentially enable harm wherein the abuser prevents them from making transactions. They could prevent any legitimate payment from going through.

Reply: Tyler Moore: That's definitely a concern. I think that's why you have to be careful in setting the threshold. My initial thoughts were something in the order of $10,000 to $15,000 – essentially a large enough amount of money that it's not met for more routine transactions or immediate needs.That's where a lot of the detail would need to be worked out.

Yangheran Piao: I think what really matters is the age distribution among the victims. The examples you gave, I don't think they're young people, right?

Reply: No, I think one was a recent retiree, and another was in her 40s.

Yangheran Piao: So maybe it should be more targeted.

Reply: There's some evidence that a lot of cybercrime victimization does skew young, especially when it comes to many of the big, rising crypto investment scams.

Luis Saavedra: My question was also related. My first reaction was also about whether these victims might want money quickly to get out of a potentially dangerous situation. But I'm not sure how that could be implemented in those cases. My second thought was that this could potentially target older citizens. But then, how would you prevent this from being seen as a loss of liberty or an admission of senility?

Reply: Well, the evidence suggests that most victims experiencing these attacks don't exhibit dementia or other age-related issues. The example of the New York Magazine columnist, for instance, is not that. However, older citizens is a community we should be very concerned about protecting. They often have the largest accounts and can experience social isolation. So, this is a community I think we certainly need to investigate ways to better protect.

Jean Martina: We're working with something very similar involving SIM card swaps. What we're trying to do is a kind of social authentication using trusted contacts. One thing we're also trying there is formal verification on those protocols, on those ceremonies, in fact. We realized there are some defenses to some of the things people spoke about regarding the contact itself. If you have a certain number of contacts, and they are randomly chosen and not available to the attacker, then it becomes safer for everybody. So instead of having only one contact, you may have two or three, and you don't control who that contact will be who is told by this person that you have some kind of contact. In our case, for reactivating your SIM card if you lose the phone, for example, it would be much safer than just going and calling the mobile phone company.

Reply: This prompts me to another idea I had, especially given the foreseeable objections to trusted contacts. Consider the case of financial trusts, where you often have to name a trustee. You can name individuals, but you can also name trust companies. You can actually name institutions that will provide that service for you. So I could also see a potential service where someone is essentially willing to be the trusted party. For a small fee, they would be willing to evaluate these transactions, give evaluations as to whether or not it's likely a scam, and then be the one to do that. This could be useful for dealing with the risk presented here, but also in cases where the trusted contact may not be in a good position to evaluate whether or not something is a scam.

Kamil Malinka: I think you should also discuss how you choose the trusted contact. We've had discussions with Czech police about phishing. We've seen many examples where people, even though they know they're under attack, still want to complete the transaction, even if the police contact them or the bank explains they're under attack. So you should probably add some extra protection so they're not able to simply remove all the good people trying to help them, just to complete the transaction.

Reply: You make a very good point. It is absolutely essential that these protections, if they are in place, cannot be easily changed during the event. That's a fundamental requirement for this scheme to work.

Luca Allodi: I think the idea you mentioned about the contact person being a third-party organization that can help actually goes in the direction of the answer here. But sometimes the bigger scams are not necessarily against people and their private funds; they're against people who control funds of other people. There was a case in Kansas, a small bank named Heartland Tri-State Bank, where the CEO was scammed, and all the bank's funds were lost because of that. So I was wondering to what extent your notion of a trusted contact can work in these scenarios, and where it would still be effective.

Reply: I think it's very clear it's not going to work for all scenarios. I think the idea is that there's very little protection right now, and it's so far from working. Let me give you another real example. My brother's Facebook account got hacked and taken over, and he couldn't get it back because the password was changed, and Facebook couldn't figure out if he was really himself. For six months, he didn't have control over his Facebook account. Eventually, the person taking over his account repurposed my brother as a cryptocurrency trader expert. He was talking about how great his life was. Then, a few weeks later, I talked to my cousin, who got a phone call from his father, my uncle, saying that my uncle thought he was dealing with my brother because he wanted to get into buying cryptocurrency, but he was actually going to a scammer instead. So these things are happening all over the place. I think enough of these scams are happening that we need to be thinking seriously about what kinds of countermeasures can be instituted to help people. Because when it happens, you lose money quickly. My uncle lost $35,000. You're definitely not going to stop everything, but we're doing so little to protect against this right now; I think we have to get started.

Jean Camp: I love the concept of the beneficiaries being notified and recognizing the need for multiple beneficiaries, and for beneficiaries to be invisible to each other, so that it doesn't trap someone. You and Richard did some work a while ago on the lifetime of phishing sites, and I wonder if there's also a lifetime for these accounts where the money is transferred to. We know there are scammer phishing wallets. If there could be account takedowns from the recipient accounts or account holds, that could complement the delay you propose. Does the same pattern exist?

Reply: I think, to some extent, that's where some of the countermeasures happen. With phishing, you'd see an ACH transfer from one banking account to the next, and those tend to be reversible. But you always want to get to it before it goes out to Western Union or one of these non-revocable payment transfers. I believe in these cases here, we also see these non-revocable payments: Western Union, MoneyGram, Bitcoin. This is where payments quickly wind up, because once criminals can get a non-reversible payment, they're home free. We could place more defenses there, but look at the advice currently given. You go to any place like Walmart in the US, and they have all these warnings about not sending money to someone you don't know, but we know those warnings don't really work, because people are usually too deep in the scam by that point. So that's why my idea is to push it further up the stack before the money can even go out.

Anton Firc: Maybe a remark that might help in designing the protocol further would be to draw inspiration from the operation of anti-fraud centers in European banks that actually do similar work. Also, an interesting practice they use is that they take notes or have a database of known fraud accounts. When a wire transfer transaction is happening to that account, they stop the transaction and get in touch with the victim. In this case, the operation is very similar to the protocol you are proposing. Additionally, there has discussion about whether banks should actually be responsible for those kinds of scams, and then they would be encouraged to take protection measures to make the users or the account holders behave responsibly.

Reply: Yes, it's interesting that the UK, as Marie Vasek pointed out to me, has some protections that have just been put in place for authorized push payments (APPs) that make financial institutions liable. It will be very interesting to observe how this plays out. My prediction is that the limits of payment sizes on those APPs are going to go way down so that banks can minimize their exposure, and scammers are going to try to stop using that as the payment method because banks are now very heavily policing it since they're on the hook for it. But in general, I think pushing more responsibility onto financial institutions makes some sense because they're in a better position to monitor. They see these patterns much more than an individual customer would.

Marie Vasek: To go a bit further on what's happening in the UK, there's been a big conversation about what's considered a bank. For instance, in the US, if you're banking with Bank of America, it's clearly a bank. But if you're sending money via Western Union, is that a bank? In the UK, if you send money to a fraudster via APP, which is how most people send money, then the bank you're part of and the bank the fraudster is part of have to split the cost 50/50. This has caused things like boutique legal actions so you can sue your bank if they decide you're actually liable for some of that fraud. But it's also starting more of a conversation about what counts as a bank for the purposes of this regulation. So if the customer pushes money to a cryptocurrency exchange, is it the responsibility of the bank that the cryptocurrency exchange uses, or is it the responsibility of that cryptocurrency exchange? This is a lot of the conversation going on right now in the UK.

Reply: Tyler Moore I wonder if maybe UK banks would be more amenable to introducing this kind of intervention or some improved version of it, because it could actually help their bottom line.