Tackling Authorised Push Payment Fraud

1 Background

An "Authorised Push Payment" (APP) fraud is a type of cyber-crime where fraudsters trick a victim into making an online payment into an account controlled by them. The "Financial Conduct Authority" (FCA) defines this type of fraud as *"a transfer of funds by person A to person B, other than a transfer initiated by or through person B, where: (1) A intended to transfer the funds to a person other than B but was instead deceived into transferring the funds to B; or (2) A transferred funds to B for what they believed were legitimate purposes but which were in fact fraudulent"* [1]. APP fraud has various variants, such as purchase, romance, investment, or invoice fraud [11]. According to a report produced by "UK Finance" *online* payment (i.e., Online Banking and cryptocurrency) is the type of payment method the victims used to make the authorised push payment in 98% of cases. Based on this report, only in the first half of 2021, a total of £355 million was lost to APP fraud, which has increased by 71% compared to losses reported in the same period in 2020 [10]. This fraud type is affecting UK residents, banks, and the economy.

Since 2016, the Payment Systems Regulator (PRS) has been collaborating with the industry and banks to improve Online Banking security and facilitate it with mechanisms that can prevent APP fraud, including two primary mechanisms (1) "Confirmation of Payee" (CoP) and (2) "Mules Insights Tactical Solution" (MITS). Briefly, CoP checks whether the details of the recipient of money (a.k.a. payee) inserted by a sender into the Online Baking platform match with the records held by the banks, and warns the sender customer if there is a mismatch [9]. CoP has been implemented by the six largest banking groups; namely, Barclays, HSBC, Lloyds Banking Group, Nationwide Building Society, NatWest, and Santander, in 2020 [12]. MITS is a technology that helps to track suspicious payments and identify those legitimate bank accounts whose owners allow their bank accounts to be used to cash out fraudulent funds; these types of accounts are called "mule counts". There has been a significant increase in online adverts persuading people to allow their bank accounts to become mule accounts. These adverts often aim at younger people who may not realise the severity of what they are doing or even know that it is a crime [9]. The amount of money lost via APP fraud and the number of cases have been significantly increasing, year on year [4]. This growth indicates that existing fraud prevention mechanisms are not effective enough. APP fraud is not specific to the UK, it has been affecting people all around the world. For instance, according to the FBI, victims of APP fraud have reported to it at least a total of $419 million in losses, in 2020 [3].

Furthermore, users of cryptocurrencies have been targets of APP fraud as well. According to the UK's "National Fraud and Cyber Crime Reporting Centre" over £146 million was lost to fraud in 2021 [8]. A report produced by the USA's "Federal Trade Commission" suggests that more than 46,000 people reported losing over $1 billion in cryptocurrency to fraud, from January 2021 through March 2022 [2]. According to this report, the top cryptocurrencies people said they used to pay fraudsters were Bitcoin (70%), Tether (10%), and Ethereum (9%). Despite the striking amount of money lost to cryptocurrency fraud, there has been no scientific approach to protect cryptocurrency users that have fallen victim to cryptocurrency fraud.

Thus, there is a pressing call for effective solutions that can deal with this type of fraud, which has been affecting people and banks in the UK and all around the world. Such an urgent need has been emphasised by the UK's "HM Treasury" very recently, in May 2022 [6].

2 Research Gaps

To deal with APP fraud, researchers and companies have developed ad-hoc mechanisms such as CoP and MITS, since 2016 when APP fraud drew the attention of regulators and banks. Nevertheless, there still exist critical research gaps; namely, **there exists no scientific study**:

- **to analyse the security of CoP**. In general, CoP is a query-response interactive protocol, where a sender of money inserts a recipient's public details (e.g., full name, and sort-code) into the Online Banking system and submits it to a bank whose responses indicate whether it has a customer with exact or similar details. Since the query can be sent by any customer including malicious ones, the CoP must ensure that the privacy of the recipient as well as other customers (that are not involved in the specific transaction with the sender of money) is not violated. However, currently, there has been absolutely no publicly available research that rigorously analyses the security of existing CoP and ensures that it does not violate money recipient's and other customers' privacy.
- **to discover mule account detection mechanisms that are agnostic to adversarial strategies**. Existing solutions that detect mule accounts rely on known adversarial behaviours. However, such solutions would be ineffective if adversaries enhance their strategies or even take advantage of sophisticated technologies, such as AI. Currently, there exists no technical solution that guarantees mule accounts can be detected without relying on known adversarial behaviours.
- **to discover a generic solution that can reimburse cryptocurrency fraud victims**. Due to the irreversible nature of transactions in cryptocurrency payment systems, and the fact that they are decentralised and do involve any central bank, it is very unlikely to recover any digital currency lost to fraud in these payment systems. Although people all around the world have been losing huge amounts of money to cryptocurrency fraud, to date, there exists no technical generic solution that can reimburse cryptocurrency fraud victims who use various cryptocurrency payment systems, e.g., Bitcoin, Tether, or Ethereum.

3 The Research Programme

3.1 The Research Aim and Questions

The overall aim of the proposal is *to find solutions that can deal with APP fraud*. This research will answer the following main questions.

Main Questions

1. *Is CoP secure? If not, how to make it provably secure?*
2. *How can we develop much stronger mule account detection mechanisms (e.g., MITS) that remain secure regardless of adversaries' strategies?*
3. *How can we devise a generic mechanism that can compensate cryptocurrency fraud victims?*

Questions 1 and 2 are fundamental. Security researchers (especially those who work on the provable security research line) ask the generalisation of these questions about any real-world security mechanisms, all the time. In this research, we ask these specific questions, because there exists no formal security definition and proof for these mechanisms (i.e., CoP and mule account detection) and the existing mule account detection mechanisms' security guarantees are dependent on adversaries' strategies. The generalisation of these questions goes back to the early 1990s when the idea of modern cryptography was proposed; the basic principles of modern cryptography state that we should (a) formally define any security mechanism's security requirements, (b) formally prove that any security mechanism meets its formal security definition, and (c) ensure that a mechanism's security guarantees are independent of specific adversarial strategies [7,5].

We ask Question 3 for two primary reasons: (a) there exists no technical mechanism that can help victims of cryptocurrency fraud receive compensation, and (b) different cryptocurrency payment systems are based on different mechanisms (e.g., different consensus protocols) and have different capabilities (e.g., some like Ethereum support arbitrary computations on transactions and some like Bitcoin does not); thus, it is vital to have a mechanism that is generic enough to support users of various cryptocurrencies that have fallen victim to cryptocurrency fraud.

References

1. Authority, F.C.: FCA glossary (2021), https://www.handbook.fca.org.uk/handbook/glossary/G3566a.html
2. Emma Fletcher: Reports show scammers cashing in on crypto craze (2022), https://www.ftc.gov/news-events/data-visualizations/data-spotlight/2022/06/reports-show-scammers-cashing-crypto-craze#crypto1
3. Federal Bureau of Investigation (FBI): Internet crime report (2020), https://www.ic3.gov/Media/PDF/AnnualReport/2020_IC3Report.pdf
4. Financial Conduct Authorty: Authorised push payment fraud (2022), https://web.cvent.com/event/f52f2d51-df03-4f4e-80ca-b90b9322f03d/websitePage:63b8425c-4cb2-409a-a51a-8b5d17ea7dc6
5. Goldreich, O.: The Foundations of Cryptography - Volume 2, Basic Applications. Cambridge University Press (2004)
6. HM Treasury: Government approach to authorised push payment scam reimbursement (2022), https://www.gov.uk/government/publications/government-approach-to-authorised-push-payment-scam-reimbursement/government-approach-to-authorised-push-payment-scam-reimbursement
7. Katz, J., Lindell, Y.: Introduction to Modern Cryptography. CRC Press (2007)
8. National Fraud and Cyber Crime Reporting Centre: Cryptocurrency fraud leads to millions in losses so far this year (2021), https://www.actionfraud.police.uk/news/cryptocurrency-fraud-leads-to-millions-in-losses-so-far-this-year
9. UK Finance: Confirmation of payee, https://web.cvent.com/event/f52f2d51-df03-4f4e-80ca-b90b9322f03d/websitePage:63b8425c-4cb2-409a-a51a-8b5d17ea7dc6, visited on: 01.07.2022
10. UK Finance: 2021 half year fraud update (2021), https://www.ukfinance.org.uk/system/files/Half-year-fraud-update-2021-FINAL.pdf
11. UK Finance: The definitive overview of payment industry fraud (2021), https://www.ukfinance.org.uk/system/files/Fraud%20The%20Facts%202021-%20FINAL.pdf
12. Which?: Confirmation of payee expansion outlined by regulator to help combat scams, https://www.which.co.uk/news/article/confirmation-of-payee-expansion-outlined-by-regulator-to-help-combat-scams-aj7LD2J9C5MY#:~:text=The%20six%20largest%20banking%20groups,Ulster%20Bank)%2C%20and%20Santander.