

## CRIMINALS TARGET ATTORNEYS WITH SCAMS INVOLVING FAKE CHECKS

Attorneys may be targeted by criminals posing as clients in need of their services to collect a debt. These schemes involve fraudulent cashiers' checks – often for very large dollar amounts – that are mailed to attorneys to pay for the false debt by criminals posing as debtors. Attorneys could be left owing thousands of dollars if they deposit the fake checks and send the "clients" funds before realizing it is a scam. In cases where the attorney is unable to cover the negative account balance caused by this scam, it might result in a loss to the financial institutions involved.

## THE SCHEME



1

A potential client contacts an attorney requesting services to recover a debt. The client provides paperwork detailing the judgment and the party who owed the debt.



3

Debtor sends the attorney a (fake) cashier's check, indicating he wants to avoid a legal dispute.



5

The client contacts the attorney, indicating the debtor informed him of the payment and asks to receive the money via wire as quickly as possible.

**Get ahead of the scam.** Funds should not be sent until the check has had time to process.





The financial institution notifies the attorney that the cashier's check was fraudulent and the funds will be removed from the client trust account.



The attorney begins working with the client to draft a demand letter to begin the collection process.

**Get ahead of the scam.** Verify the paperwork, debt amount and other details through reputable independent sources.



When the cashier's check is received in the mail, the attorney deposits it into the client trust account.



Based on the client's request, the attorney wires the funds to the client, minus the attorney's fees.



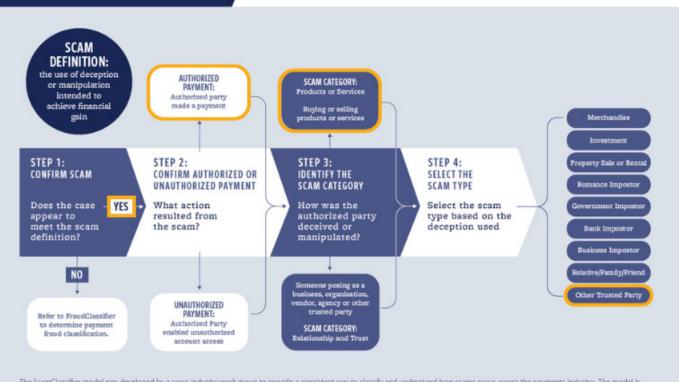
"The "client" and "debtor" disappear, and the attorney loses the money that was wired to the "client."

## CRIMINALS TARGET ATTORNEYS WITH SCAMS INVOLVING FAKE CHECKS

Identifying and classifying these scams can help financial institutions track trends, shift resource allocation and educate stakeholders to improve awareness and help prevent future scams.



The ScamClassifer<sup>SM</sup> model supports consistent and detailed classification, reporting, analysis and identification of trends in scams. It uses a series of questions to differentiate and classify scams by categories and types, and provides a view of the full impact of scams by including cases that resulted in authorized payments, as well as unauthorized payments from account access. The model also can be used to capture attempted scams.



The ScamClassifier model was developed by a cross-industry work group to provide a consistent way to classify and understand how scams occur across the payments industry. The model is not intended to result in mandates or regulations, and does not give any legal status, rights or responsibilities, nor is it intended to define or imply liabilities for loss or create legal definitions, regulatory or reporting requirements. While sharing and use of the ScamClassifier model throughout the industry is encouraged, any adoption of the ScamClassifier model is voluntary at the discretion of each individual entity. Absent written consent, the ScamClassifier model may not be used in a manner that suggests the Federal Reserve endorses a third-party product or service.

The check fraud mitigation toolkit was developed by the Federal Reserve to help educate the industry about check fraud and outline potential ways to help detect and mitigate this fraud type. Insights for this toolkit were provided through interviews with industry experts, publicly available research, and team member expertise. This toolkit is not intended to result in any regulatory or reporting requirements, imply any liabilities for fraud loss, or confer any legal status, legal definitions, or legal rights or responsibilities. While use of this toolkit throughout the industry is encouraged, utilization of the toolkit is voluntary at the discretion of each individual entity. Absent written consent, this toolkit may not be used in a manner that suggests the Federal Reserve endorses a third-party product or service.