ICBA
One Mission. Community Banks.

Combating Crypto-Enabled Scams: The Community Bank Perspective

The Independent Community Bankers of America, representing community banks across the nation with nearly 50,000 locations, appreciates the opportunity to provide this statement for the record for today's hearing: "Protecting Americans' Savings: Examining the Economics of the Multi-Billion Dollar Romance Confidence Scam Industry."

As we discuss in this statement, community banks are concerned with the rise of romance confidence scams and are committed to protecting their customers and their institutions from scams of all kinds, but they can't do it alone. To stop these scammers, we need social media, dating, and telecom companies to do more to prevent these scammers from contacting potential victims and the support of Congress, agencies, and international institutions acting in coordination. Additionally, it is important to address how these scams are facilitated by cryptoassets, decentralized finance (DeFi) applications, and critical gaps in the financial regulatory system.

This statement will describe the workings and the scope of romance confidence scams. This scam is of interest primarily because it illustrates and exemplifies the hazards of unregulated crypto for consumers and the banking system. We discuss recommended safeguards for consumers and the banking system to reduce the incidence of this scam.

Romance Confidence Scams Are a Growing Concern

Romance confidence scams have climbed sharply in recent years as transnational criminal syndicates largely based in Southeast Asia use online channels to target consumers and communities served by community banks. These scams are also commonly known as "pig butchering," likening the victim to a pig being fattened for slaughter.

Scammers create fictitious personas—possibly employing deepfake images—to establish contact with potential victims, typically by text messages, social media, or dating apps. Over time, a scammer fosters seemingly authentic relationships with victims through frequent and friendly or flirtatious exchanges. Eventually, the scammer will raise the topic of cryptocurrencies and the investment opportunities they offer. Rather than ask for money or cryptocurrency directly, the scammer will guide a victim's investment strategies and instruct them to send money to various platforms (which are developed or controlled by the scammer).

Scammers present false account information purportedly showing victims' investments are growing and continue to pressure victims to send money until they are "bled dry." It is not uncommon for victims to try to cash out their investments only to be told that they must first pay exorbitant fees or taxes. By this point, the scam has run its course, the money is gone, and scammers have moved on to their next victims. Tragically, there are countless stories of victims losing their entire life savings to these schemes.

The estimated scale of this fraud exceeds many other major financial crimes, including business email compromise. In fact, the FBI's 2023 Internet Crime Complaint Report revealed that investment scams claimed the most substantial losses of all crimes tracked by the agency. Last year, losses soared 38 percent to reach $4.57 billion, with crypto-related investment fraud accounting for almost 90 percent of that total.

866-843-4222
icba.org
1615 L Street NW
Suite 900
Washington, DC 20036
518 Lincoln Road
P.O. Box 267
Sauk Centre, MN 56378

However, these figures only reflect the losses reported to law enforcement; the true toll is likely much higher. Researchers at the University of Texas said romance confidence scams have netted at least $75.3 billion since January 2020, and they conceded that their analysis could fall short of the total. Whatever the genuine number may be, the impact is undeniable: Scammers are successfully seizing vast sums of money from numerous victims, and crypto serves as the primary conduit for their illicit gains.

The Role of Crypto, Tether and Decentralized Exchanges

Romance confidence scams depend on cryptocurrencies to function. But the connections between crypto and this skyrocketing scam run much deeper than the fake investments that ensnare consumers. Cryptocurrency also serves as the favored payment method for scammers, and the wider crypto ecosystem enables an underground financial system to help launder their proceeds. Given these fundamental risks, policymakers must act to strengthen anti-money laundering requirements for crypto entities, including those that claim to be decentralized.

According to new research from the University of Texas, the Tether stablecoin is the predominant payment mechanism, accounting for 84 percent of the total volume of transactions associated with crypto addresses tied to scammers. Likewise, the United Nations found that Tether issued on the Tron blockchain is a "preferred choice for regional cyberfraud operations and money launderers alike" due to its stability and the ease, anonymity, and low fees of its transactions. As bearer instruments, stablecoins have no anti-money-laundering or know-your-customer checks after they enter circulation, and they are easily transferred between unhosted wallets.

Additionally, the University of Texas study found that scammers frequently use decentralized exchanges to trade one cryptoasset for another. In a report published last year, Treasury said criminals are attracted to DeFi due the complete lack of customer identification processes, and it acknowledged that these "laundering methods can create challenges for investigators attempting to trace illicit proceeds."

Community Bank Efforts

Community banks make every effort to enable their customers to safely conduct transactions. This includes continually educating their customers and employees about the latest scams and warnings from bank regulators, law enforcement and national security professionals.

Community banks continue to make significant strategic investments in fraud and scam prevention and detection. They have also worked to revisit policies and procedures to streamline mitigation efforts and comply with a complex set of regulations. As a result, community banks are increasingly resilient against fraudsters. Community banks also provide educational resources to empower customers and, when fraud occurs, effective partnership to help them recover.

Unfortunately, a romance confidence scam, by design, preys on the aspirations of its victim and overrides their judgement. It can be nearly impossible to convince a customer that they are a victim until it becomes too late. We urge policymakers to focus their attention on the source of the problem: the cryptocurrency industry.

Policymakers Must Act

The persistent growth of romance confidence scams emphasizes the urgent need for greater regulation across the cryptocurrency ecosystem**.** ICBA urges policymakers to prioritize national security and counter the illicit activities enabled by cryptocurrency.

ICBA is troubled by the regulatory gaps found throughout the growing world of DeFi. We support the Internal Revenue Service's proposal to require decentralized crypto trading platforms to conduct proper KYC to obtain the necessary information for digital asset tax-reporting requirements. Requiring DeFi exchanges to collect such information could also provide law enforcement with vital data to help track criminal activity throughout the

crypto ecosystem, particularly the increasingly frequent large-scale hacks and money laundering conducted by state-sponsored groups and foreign criminal enterprises.

ICBA also appreciates efforts taken by the Financial Crimes Enforcement Network in their notice of proposed rulemaking to classify all transactions involving cryptocurrency mixers—a broad term describing various technologies that shroud key transactional details—as a "primary money laundering concern" and mandate enhanced reporting and recordkeeping by financial institutions. Mixers are frequently used by cybercriminals to cover their tracks after they steal cryptoassets or obtain ransoms paid in crypto.

The government has tried to curb the use of mixers with penalties against the major operators, but bad actors routinely flout any limitations. While FinCEN's proposal marks a significant step forward, it is fundamentally inadequate to address the potent threat posed by mixers. ICBA believes FinCEN needs to strengthen its efforts by recognizing the equally important roles that DeFi exchanges, bridges, and unhosted wallets play in money laundering operations. Regulators must address how these platforms are used in the money laundering process. Actions against mixers alone are not enough to curtail criminal activity.

International Efforts Needed

ICBA also recognizes that FinCEN cannot solve all the problems stemming from the crypto ecosystem. The growth of romance confidence scams originating from other countries underscores the critical need for the U.S. government to help lead an international effort to reinforce and harmonize digital assets regulatory frameworks around the world.

International partnerships with financial institutions, law enforcement, national security organizations, and regulators are essential to succeed in this mission. To that end, ICBA continues to advocate for digital assets regulation that addresses the myriad risks associated with cryptoassets with important international bodies, including in comment letters to the International Organization for Securities Commissions and the Financial Stability Board.

Closing

Thank you for convening this hearing and raising the profile crypto-enabled scams to consumers and the banking system.