Pig Butchering—How Financial Institutions Can Strengthen Their Compliance Programs to Mitigate Potential Liability

Wednesday, August 5, 2025

EXECUTIVE SUMMARY

Cryptocurrency-related scamming poses a growing risk to financial institutions and their customers. According to Chainalysis, customers worldwide lost an estimated $17 billion in crypto scams and fraud in 2025, a significant increase from the roughly $12 billion lost per year from 2021-2024.[1] Cryptocurrency investment fraud, commonly known as "pig butchering," represents the greatest individual category of financial loss: in 2025, Americans lost approximately $7.2 billion to pig butchering schemes.[2]

Pig butchering scams are also attracting considerable attention from federal agencies. For example, in October 2025, the Department of Justice (DOJ) and the Office of Foreign Assets Control (OFAC) announced substantial parallel actions against alleged pig butchering enterprise Prince Holding Group and its purported leader Chen Zhi:[3] the DOJ seized $15 billion in bitcoin allegedly controlled by Prince Holding Group, while OFAC sanctioned 25 crypto wallets allegedly linked to Zhi in the amount of $780

---

[1] Based on historical trends, Chainalysis estimated that the amount will grow by roughly 24% as it identifies more illicit wallet addresses. Chainalysis Team, *Record $17 Billion Estimated Stolen in Crypto Scams and Fraud in 2025 as Impersonation Tactics and AI Enablement Surge*, Chainalysis (Jan. 13, 2026), https://www.chainalysis.com/blog/crypto-scams-2026/.

[2] *See* Fed. Bureau of Investigation, *2025 IC3 Annual Report* 11 (2025), https://www.ic3.gov/AnnualReport/Reports/2025_IC3Report.pdf.

[3] Zhi was later arrested by Cambodian authorities on January 6, 2026, and subsequently transferred to Chinese authorities. Because Chinese law bars the extradition of its own citizens and China has no extradition treaty with the U.S., it is unlikely that Zhi will be extradited to the U.S. John Annese, *Crypto Kingpin Charged with Fraud in NYC is Arrested in Cambodia, Deported to China*, Daily News (Jan. 7, 2026, at 15:15 ET), https://www.nydailynews.com/2026/01/07/crypto-fraud-kingpin-charged-nyc-indictment-busted-cambodia-deported-china/.

million and added Zhi and others to its Blocked Persons List.[4] Additionally, the Federal Bureau of Investigation, the DOJ, and the U.S. Attorney's Office for the District of Columbia have launched the Scam Center Strike Force—a task force focused on prosecuting cryptocurrency scams that are "creating a generational wealth transfer from Main Street America into the pockets of Chinese organized crime."[5] Furthermore, other regulators are warning financial institutions and consumers about these scams.[6] Finally, President Trump recently published an Executive Order ordering "[t]he Secretary of State, the Secretary of the Treasury, the Secretary of War, the Attorney General, and the Secretary of Homeland Security" to review how their departments can combat scam centers and cybercrimes committed by transnational criminal organizations.[7]

This article explains the rising danger pig butchering may present to financial institutions and their customers and offers insight into how financial institutions can help prevent pig butchering and/or mitigate related liability in customer lawsuits.

WHAT IS PIG BUTCHERING?

The term pig butchering originates from the scam's resemblance to the fattening of a pig for slaughter: first, the scammer "fattens" the victim by drawing the victim in using a false pretense, often in the nature of a personal or romantic relationship. Then, leveraging the personal bond that the victim believes has formed, the scammer induces the victim to contribute increasing amounts of money into a faux investment scheme. Finally, the scammer "butchers" the victim by ending the relationship and taking all of the victim's deposits.[8] Pretending to be interested

---

[4] *See* Press Release, U.S. Dep't of Justice, Chairman of Prince Group Indicted for Operating Cambodian Forced Labor Scam Compounds Engaged in Cryptocurrency Fraud Schemes (Oct. 14, 2025), https://www.justice.gov/opa/pr/chairman-prince-group-indicted-operating-cambodian-forced-labor-scam-compounds-engaged (announcing the unsealing of Zhi's criminal indictment); Tim Craig, *'Pig Butchering' Kingpin's $780m Bitcoin Sanctioned by OFAC*, Yahoo Finance (Oct. 31, 2025), https://finance.yahoo.com/news/pig-butchering-kingpin-780m-bitcoin-165619259.html; Press Release, U.S. Off. of Foreign Assets Control, Transnational Criminal Organizations Designations; Issuance of TCO-related General License (Oct. 14, 2025), https://ofac.treasury.gov/recent-actions/20251014.

[5] Press Release, U.S. Dep't of Justice, New Scam Center Strike Force Battles Southeast Asian Crypto Investment Fraud Targeting Americans (Nov. 12, 2025), https://www.justice.gov/usao-dc/pr/new-scam-center-strike-force-battles-southeast-asian-crypto-investment-fraud-targeting.

[6] *See* Press Release, Fin. Crimes Enf't Network, FinCEN Reminds Financial Institutions of Its Resources on Identifying Potential Relationship Scams (Feb. 13, 2026), https://www.fincen.gov/news/news-releases/dating-or-defrauding-2026; Press Release, Commodity Futures Trading Comm'n, CFTC Targets Relationship Investment Scams with National and International Initiatives the Valentine's Week (Feb. 9, 2026), https://www.cftc.gov/PressRoom/PressReleases/9181-26; *see also* Consumer Alert, Off. of the N.Y. State Att'y Gen., Attorney General James Warns New Yorkers About "Pig Butchering" Scams (Feb. 17, 2026), https://ag.ny.gov/press-release/2026/attorney-general-james-warns-new-yorkers-about-pig-butchering-scams.

[7] Exec. Order No. 14390, Combating Cybercrime, Fraud, and Predatory Schemes Against American Citizens (Mar. 6, 2026), https://www.whitehouse.gov/presidential-actions/2026/03/combating-cybercrime-fraud-and-predatory-schemes-against-american-citizens/.

[8] *See* Cezary Podkul, *How Foreign Scammers Use U.S. Banks to Fleece Americans*, ProPublica (June 25, 2025, at 05:00 ET), https://www.propublica.org/article/pig-butchering-scam-cybercrime-us-banks-money-laundering; Fin. Crimes Enf't

in business opportunities, friendship, or romance, scammers initially target potential victims through text messages, online dating profiles, and various social media platforms.[9] In a common formulation of pig butchering, once a scammer has gained a victim's trust, the scammer transitions the conversation to encrypted messaging, introduces the idea of investing in cryptocurrency, and coaxes the victim into investing on phony or imposter platforms that appear legitimate.[10] The scammer then manipulates these fake platforms to show the victim fake returns, and, at times, allows small withdrawals to appear legitimate and encourage future investment.[11] When the scammer believes the victim has lost the willingness or ability to make further investments, the scammer severs the relationship and pockets the victim's entire investment.[12]

Although confidence and investment scams are nothing new, organized pig butchering enterprises are a recent phenomenon. During the COVID-19 pandemic, Chinese criminal networks repurposed empty casinos in Southeast Asia into forced-labor scam compounds.[13] For example, the DOJ's indictment of Zhi alleges that Prince Holding Group operated at least ten of these compounds across Cambodia where workers engaged in cryptocurrency fraud schemes resulting in billions of dollars in losses to victims worldwide.[14] Recent studies report as many as 300,000 scammers operating in "industrial-scale forced-labor" scam compounds in Cambodia, Laos, and Myanmar.[15] These scammers are often lured to the scam compounds via elaborate recruitment campaigns promising legitimate employment opportunities in foreign locales. This recruitment often includes multiple rounds of online interviews and a free plane ticket to Southeast Asia—with candidates arriving at the destination only to discover that they cannot leave and are forced to join the criminal enterprise.[16]

Pig butchering is here to stay: cyber scamming has become highly profitable in Southeast Asia and is alleged to be protected by ruling elites.[17] In one documented instance, the mayor of a municipality in the Philippines helped a scamming enterprise obtain permits and allowed it to house more than 800 foreign workers in a compound on her property.[18] According to Jacob Sims, an expert on transnational and cybercrime in the region, scamming in Laos, Cambodia, and Myanmar has exploded over the last five years, evolving from "small online fraud rings into an

---

Network, *FinCEN Alert on Prevalent Virtual Currency Investment Scam Commonly Known as "Pig Butchering"* 1 (FIN-2023-Alert005, Sep. 8, 2023), https://www.fincen.gov/system/files/shared/FinCEN_Alert_Pig_Butchering_FINAL_508c.pdf (explaining that the term also derives from a Chinese term that roughly translates to pig butchering).

[9] *See Crypto Investment Scams*, Am. Bankers Ass'n (Sep. 11, 2024), https://www.aba.com/news-research/analysis-guides/crypto-investment-scams.

[10] *See id.*

[11] *See id.*

[12] *See* FinCEN Alert, *supra* note 8.

[13] *See* U.S. Inst. of Peace, *Transnational Crime in Southeast Asia* 8, 18 (May 2024), https://www.usip.org/sites/default/files/2024-05/ssg_transnational-crime-southeast-asia.pdf.

[14] *See* Indictment ¶¶ 1, 31, *United States* v. *Zhi*, No. 25-CR-312 (E.D.N.Y. Oct. 8, 2025).

[15] *See* U.S. Inst. of Peace, *supra* note 13; *Hundreds of Thousands Trafficked into Online Criminality Across SE Asia*, United Nations (Aug. 29, 2023), https://news.un.org/en/story/2023/08/1140187#:~:text=Criminal%20gangs%20in%20southeast%20Asia,countries%20of%20destination%20or%20transit.

[16] *See* U.S. Inst. of Peace, *supra* note 13.

[17] *See id.* at 9, 33.

[18] *See* Francesca Regalado, *Ex-Mayor Is Sentenced to Life for Human Trafficking Tied to Scam Centers*, N.Y. Times (Nov. 20, 2025), https://www.nytimes.com/2025/11/20/world/asia/alice-guo-life-sentence-philippines.html.

industrial-scale political economy."[19] These criminal networks have arguably become dominant national political and economic engines, resulting in their countries being called "scam states."[20]

THE RESPONSIBILITIES AND POTENTIAL LIABILITY OF FINANCIAL INSTITUTIONS IN CONNECTION WITH PIG BUTCHERING

As gatekeepers of the financial system, financial institutions have a responsibility under the Bank Secrecy Act (BSA) to maintain sufficient compliance programs to combat money laundering.[21] This includes continually updating anti-money laundering (AML) compliance programs to keep pace with contemporary risks like pig butchering scams, which present unique challenges. For example, in a pig butchering scam, the victim—not the fraudster—authorizes each transaction. And because victims are so frequently and intensely manipulated by scammers who establish trust prior to introducing financial opportunities, victims themselves often circumvent attempts by banks to prevent these fraudulently induced transactions.[22] Seduced by "easy money" and other motivations, victims may even switch banks if they fear additional transactions will not be authorized, or if previous transactions have been denied.[23] According to one recently filed complaint in federal district court in California, a retired anesthesiologist voluntarily wired $7.9 million into two separate pig butchering schemes, with the majority of wire transfers occurring at a second bank after the first bank refused to process any additional wires.[24]

For years there have been special directives to financial institutions to flag pig butchering. Financial institutions must file Suspicious Activity Reports (SARs) whenever they know, suspect, or have reason to suspect that a completed or attempted transaction involves funds derived from illegal activity.[25] The Financial Crimes Enforcement Network (FinCEN) requires financial institutions to include the term "FIN-2023-PIGBUTCHERING" in pig butchering-related SARs, and FinCEN has provided a list of fifteen red flags/indicators to assist financial institutions in evaluating potential pig butchering transactions and building their compliance programs.[26] Some of these red flags include accounts experiencing abrupt, continuous change in their baseline withdrawal or wiring activity; customers receiving large loans and immediately using the loan proceeds to purchase cryptocurrency; repeated access attempts from IP addresses, devices, and geographies that are inconsistent with historical account activity; small test transactions followed by substantially larger ones; transaction notes indicating that the transaction is related to taxes, penalties, or fees; and customer comments indicating customers' lack of

---

[19] Tess McClure, *Age of the 'Scam State': How an Illicit, Multibillion-Dollar Industry Has Taken Root in South-East Asia*, The Guardian (Dec. 1, 2025, at 21:02 ET), https://www.theguardian.com/technology/2025/dec/02/scam-state-multi-billion-dollar-industry-south-east-asia.
[20] *See id*.
[21] *See Bank Secrecy Act/Anti-Money Laundering (BSA/AML)*, Fed. Deposit Ins. Corp. (Feb. 6, 2026), https://www.fdic.gov/banker-resource-center/bank-secrecy-act-anti-money-laundering-bsaaml.
[22] *See* ProPublica, *supra* note 8.
[23] *See id*.
[24] *See* Second Am. Compl. ¶¶ 4, 31, *Lee* v. *HSBC Bank USA, N.A.*, No. 2:26-cv-01198 (C.D. Cal. May 26, 2026).
[25] *See* FinCEN Alert, *supra* note 8.
[26] *See id.* at 8.

understanding of cryptocurrency yet concurrent desire to invest in suspicious cryptocurrency investment schemes.[27]

The rise of significant losses from pig butchering scams has led to customer-victims filing lawsuits against the financial institutions that processed the victims' transactions. After losing a substantial portion of their finances to an unknown scammer, victims attempt to recover from likely innocent but known third parties: the banks that processed or received the fraudulent transactions. However, most victim-plaintiffs struggle to surpass the motion to dismiss stage due to their inability to plead facts illustrating that a bank had actual knowledge of fraud afoot.[28]

Processing transactions despite multiple red flags increases the odds that a judge will impute knowledge to a bank—even though a customer knowingly authorized the transactions. In at least one instance, a court allowed a case to advance beyond the motion to dismiss stage because particular facts permitted the imputation of actual knowledge to a bank.[29] Specifically, in *Lin* v. *JPMorgan Chase Bank, N.A.*, the court imputed knowledge to Chase Bank because the same employee at the same branch processed six of the plaintiff's highly unusual, quick-succession wire transfers, which led the court to conclude that the employee must have known that the plaintiff was the victim of a scam.[30] The court further reasoned that "[c]ircumstantial evidence tending to show that a reasonable person would have known [a fact]" would "likewise tend to show that a particular defendant was aware of that fact."[31]

The bounds of a financial institution's liability will be further tested in *Lee* v. *HSBC Bank USA, N.A.* In this case, the victim's son and daughter each separately alerted bank employees—in person and via telephone—that their father was a victim of a pig butchering scheme, which led to the bank temporarily freezing his account yet subsequently authorizing $2.2 million in wire transfers in the ensuing months.[32]

CONTROLS TO MITIGATE PIG BUTCHERING LIABILITY FOR FINANCIAL INSTITUTIONS

Although unmentioned in FinCEN's list of red flags, flagging of transactions that are implausibly higher than those typical in the receiver's country of residence may be a helpful component of a pig butchering prevention and detection compliance program. Both can help detect money mules like those at Virtual Asset Service Providers,

---

[27] *See id.* at 5-6.
[28] *See, e.g.*, *Lee* v. *Foris DAX, Inc.*, 2025 WL 2578239, at *1, *3, *5-7 (N.D. Cal. Sep. 5, 2025) (holding that the plaintiff failed to show that Crypto.com had actual knowledge of the torts or substantially assisted in their commission and thus dismissed the aiding and abetting fraud and receipt of stolen property claims); *Richter* v. *KRG Trading, Inc.*, 2025 WL 2371807, at *2, *4, *6 (C.D. Cal. July 10, 2025) (holding that the defendants' receipt and transfer of funds, "while important, [were] not a 'substantial factor in the sequence of responsible causation'" and "[a]t bottom, the fact that the [d]efendants turned a blind eye to certain fraudulent transactions [did] not support the inference that they necessarily agreed to facilitate or be a part of the pig butchering scheme").
[29] *See Lin* v. *JPMorgan Chase Bank, N.A.*, 2024 WL 5182199, at *5 (C.D. Cal. Aug. 15, 2024). The case was subsequently resolved at a September 12, 2025, settlement conference. *See* Minutes of Settlement Conference, *Lin* v. *JPMorgan Chase Bank, N.A.*, No. 2:24-cv-01837 (C.D. Cal. Sep. 12, 2025).
[30] 2024 WL 5182199, at *7 (C.D. Cal. Aug. 15, 2024).
[31] *Id.*
[32] *See* Second Am. Compl. ¶¶ 17-18, 28-29, *Lee* v. *HSBC Bank USA, N.A.*, No. 2:26-cv-01198 (C.D. Cal. May 26, 2026).

who have reused common KYC information such as residential addresses.[33] Follow-on IP addresses may be inconsistent with this reused-KYC information (i.e., accessing an account via a Cambodian-based VPN but providing a U.S. residential address), and mule accounts may share similar IP addresses.[34] Taking a geographically risk-based approach, financial institutions should exercise particularly heightened vigilance relating to transactions to Southeast Asia in amounts substantially larger than the average wages in the region. Plaintiffs have cited this irregularity specifically in recent litigation against financial institutions. For example, in one complaint, a plaintiff stated "[a]t no time [did] the [the bank] ever ask Plaintiff additional questions, such as why his friend who needed help in Vietnam required more than the equivalent of what an average person in Vietnam earns over the course of their entire lifetime sent to several different people."[35]

In addition, financial institutions should consider how best to update their compliance programs with artificial intelligence (AI) technology to enhance their ability to detect and act on these red flags.[36] Meta, although not a financial institution, recently announced new account protections aimed at flagging suspicious activity, including warning users about suspicious friend requests and offering users the ability to submit recent chat messages for AI scam review. Meta further shared some of the proactive steps it has taken to interdict scam operations: in 2025, Meta removed over 159 million scam ads and 10.9 million Facebook and Instagram accounts associated with scam centers.[37] Although financial institutions lack an affirmative obligation to root out fraud, there is a lesson to be learned here: it may be good business to take steps to reduce the ability of scammers utilizing banking services for nefarious activities.[38]

Even though customers in the midst of being scammed may simply close their account and take their funds to the bank next door, banks should evaluate certain enhanced controls to prevent their platforms from being used to conduct fraudulent transactions. When considering an effective framework, key aspects may include robust KYC programs that incorporate data analytics and AI-powered tools to detect commonly reused information, monitor

---

[33] *See Elliptic's Typologies Report: Detecting the Money Flows Behind the Global Pig Butchering Ecosystem*, Elliptic (Oct. 17, 2025), https://www.elliptic.co/blog/elliptics-typologies-report-detecting-the-money-flows-behind-the-global-pig-butchering-ecosystem.
[34] *See id*.
[35] Compl. ¶ 52, *Harris* v. *Wells Fargo Bank, N.A. et al*., No. 4:25-cv-00027 (S.D. Iowa Jan. 24, 2025). This was also reported in the media, *see* Clark Kauffman, *Iowa Man Sues Over $716,212 Loss in Alleged Cryptocurrency Scam*, Yahoo News (Jan. 28, 2025, at 16:54 ET), https://www.yahoo.com/news/articles/iowa-professor-sues-over-716-215449334.html.
[36] *See Innovation at the Speed of Markets: How Regulators Keep Pace with Technology: Hearing Before the Subcomm. on Dig. Assets, Fin. Tech. & A.I. of the H. Comm. on Fin. Servs.*, 119th Cong. (2026) (statement of Ryan Billingsley, Director, Div. of Risk Mgmt. Supervision, Fed. Deposit Ins. Corp.), https://www.fdic.gov/news/speeches/2026/innovation-speed-markets-how-regulators-keep-pace-technology-0 ("We are seeing firsthand how banks are adopting a range of technologies . . . . Banks have increasingly utilized AI and machine learning in a range of areas, including fraud detection, anti-money laundering and countering the financing of terrorism (AML/CFT) processes, and credit underwriting.").
[37] *See Fighting Scammers and Protecting People with New Technology and Partnerships*, Meta (Mar. 11, 2026, at 10:35 ET), https://about.fb.com/news/2026/03/fighting-scammers-protecting-people-with-new-technology-and-partnerships/.
[38] Meta also helped coordinate "Disruption Week," which led to several private sector corporations voluntarily freezing over $3.8 million in stolen cryptocurrency. *See* Sydney Price, *DOJ Says Meta and Others Froze $3.8M Tied to Crypto Fraud*, Law360 (June 4, 2026, at 20:38 ET), https://www.law360.com/fintech/articles/2485840/doj-says-meta-and-others-froze-3-8m-tied-to-crypto-fraud.

customer behavior, and detect off-baseline activity.[39] In addition, financial institutions may implement and maintain robust education programs to hone employees' abilities to detect pig butchering red flags, as well as increase customer awareness to reduce the likelihood of customers falling victim to these types of scams.[40] Banks may often be well-served to employ smart friction measures—moments where pauses are necessary to aid customer decision making—to caution customers about scams before authorizing a transfer, especially for customers who have never wired money before and are attempting to authorize a large transaction.[41]

One notable example of a financial institution taking such proactive steps is in the case of JPMorgan Chase. In November 2025, the bank announced a fraud and scam prevention initiative through which the bank hosted 20 free educational workshops to educate the public on how to recognize and avoid falling victim to scams.[42] Chase also shared some of its successful prevention tactics, including: sending scam warnings to customers when advanced technology detects suspicious transactions; enabling customers to designate a trusted contact who may be notified of certain transactions on the customer's account; developing a dedicated Scam Interruption team that works to stop scams in real time and provides support for customers; utilizing an Elderly and Vulnerable Person team to assist vulnerable adults who are more likely to become victims of financial abuse; continually educating Chase bankers on the latest scam trends; and coordinating with law enforcement.[43] Collectively, these measures have the potential to reduce fraud and increase customer awareness and institutional trust.[44]

---

[39] *See* Vail Herard, *Why Smart Financial Institutions Treat Compliance as a Competitive Advantage*, ProSight Fin. Ass'n (July 24, 2025), https://www.prosightfa.org/insights/why-smart-financial-institutions-treat-compliance-as-a-competitive-advantage/; *see also* KPMG & Chainalysis, Crypto Risk and Opportunities: A New Banking Paradigm 5 (Mar. 2025), https://assets.kpmg.com/content/dam/kpmg/ng/pdf/2025/03/Crypto%20Risk%20and%20Opportunities_A_New%20Banking%20Paradigm%20March%2010%20update.pdf ("For financial institutions, [the rise in crypto scams] signals a fundamental shift in legacy financial crime typologies, thus, challenging traditional financial monitoring systems."); *id.* at 7 ("By integrating blockchain analytics into their compliance frameworks, forward thinking banks and other financial institutions would enhance their ability to detect illicit finance, expand into new financial services, and position themselves at the forefront of an increasingly digital financial system.").

[40] *See, e.g.*, Terri Luttrell, *Crypto Scams and Crypto Fraud Detection for Financial Institutions*, Colo. Banker Mag. (Mar. 28, 2025), https://colorado-banker.thenewslinkgroup.org/crypto-scams-and-crypto-fraud-detection-for-financial-institutions/ (discussing how financial institutions can help prevent clients from falling victim to cryptocurrency-related scams); *The Snowballing Scam That's Out to Slaughter Your Savings*, M&T Bank, https://www.mtb.com/library/article/pig-butchering (posting a customer awareness message).

[41] *See* Alex Kreger, *Friction in Digital Banking Is a Feature, Not a Bug*, Forbes (Dec. 27, 2024, at 08:45 ET), https://www.forbes.com/councils/forbesbusinesscouncil/2024/12/27/friction-in-digital-banking-is-a-feature-not-a-bug/; *JPMorganChase Announces Largest Financial Fraud and Scam Prevention Effort in Firm's History*, Chase (Nov. 17, 2025), https://media.chase.com/news/jpmc-announces-largest-financial-fraud-and-scam-prevention-effort-in-firms-history; EY, Unveiling the Impact of Scam Categorization: Forensic & Integrity Services 2 (Aug. 2024), https://www.ey.com/content/dam/ey-unified-site/ey-com/en-us/insights/forensic-integrity-services/documents/ey-us-forensics-unveiling-the-impact-of-scam-categorization.pdf ("Institutions should alert their customers to red flags like forceful sales, unknown requesters, emotional pressure and demands for sensitive information . . . . Adding additional controls such as text confirmations, daily limits, extra verification[,] and additional friction for atypical payment requests can further shield customers from potential losses.").

[42] *See* Chase, *supra* note 41.

[43] *See id.*

[44] *See* Forbes, *supra* note 41.

Financial institutions must also monitor for changing regulatory norms. For example, on April 7, 2026, FinCEN announced a Notice of Proposed Rulemaking intended to "fundamentally reform" financial institutions' AML and countering the financing of terrorism (CFT) programs under the BSA.[45] These reforms include, but are not limited to, refocusing compliance obligations and expectations on effectiveness by distinguishing between deficiencies resulting from program design ("establishment") and implementation ("maintenance"); empowering financial institutions to direct more attention and resources toward higher-risk customers and activities; and clarifying expectations of independent testing and audit functions and risk-based programs.[46] The proposed rule also requires that financial institutions establish a risk-based program that incorporates "four core required pillars: (1) internal policies, procedures, and controls, including risk assessment processes, and, when applicable, ongoing customer due diligence; (2) independent program testing; (3) designation of a U.S.-based compliance officer; and (4) ongoing employee training."[47] Additionally, the proposed rule notes that when FinCEN weighs whether to pursue an enforcement or a significant supervisory action, or reviews a proposed supervisory action by a federal banking supervisor, FinCEN's director would consider whether the financial institution is employing innovative tools such as AI that demonstrate the effectiveness of that institution's AML/CFT program.[48] While the rule is not finalized, it is obvious that regulators expect financial institutions to dedicate resources to both (1) ongoing employee training and (2) incorporating AI and other emerging technologies into their AML/CFT programs.[49]

Given the evolving regulatory framework and lessons learned from recent cases, financial institutions should implement appropriate risk-based, technology-driven fraud prevention frameworks that are reasonably designed to identify, interrupt, and report scam activity—particularly pig butchering schemes—across the full customer lifecycle. This framework can include dynamic risk assessments that explicitly account for cryptocurrency-related fraud, transactional and behavioral monitoring systems calibrated to detect red flags like signs of customer coercion or distress, and real-time intervention protocols such as customer outreach and escalation procedures when high-risk activity is identified. Taken together, these measures can form a reasonably designed system that is operationally effective in detecting and mitigating fraud before losses occur.

CONCLUSION

Financial institutions must ensure compliance programs are structured to evolve so that these programs remain effective in an ever-changing environment. The lawsuits to date have only rarely survived the motion to dismiss stage of litigation, but these outcomes could evolve as more lawsuits are filed and/or courts decide to impute actual knowledge to banks due to plausible allegations of lackluster compliance efforts. As the federal government

---

[45] Press Release, Fin. Crimes Enf't Network, FinCEN Proposes Rule to Fundamentally Reform Financial Institution Programs Designed to Fight Illicit Finance (Apr. 7, 2026), https://www.fincen.gov/news/news-releases/fincen-proposes-rule-fundamentally-reform-financial-institution-programs.

[46] *See* Fin. Crimes Enf't Network, *Fact Sheet: Proposed Rule to Fundamentally Reform Financial Institution AML/CFT Programs*, https://www.fincen.gov/system/files/2026-04/Program-NPRM-FactSheet.pdf.

[47] *Id.*

[48] *See id.*

[49] *See generally* Anti-Money Laundering and Countering the Financing of Terrorism Programs, 91 Fed. Reg. 18704 (Apr. 10, 2026) (to be codified at 31 C.F.R. pts. 1010, 1020-1030), https://www.federalregister.gov/documents/2026/04/10/2026-07033/anti-money-laundering-and-countering-the-financing-of-terrorism-programs.

increases its efforts to dismantle pig butchering networks and general awareness of these scams continues to grow, both the government and the public will continue to pay attention to financial institutions' involvement in these ecosystems.

* * *

If you have any questions about the issues addressed in this memorandum, or if you would like a copy of any of the materials mentioned in it, please do not hesitate to call or email authors Brock Bosson (partner) at 212.701.3136 or Bbosson@cahill.com; Frank Weigand (partner) at 212.701.3890 or Fweigand@cahill.com; Sarah Marron (associate) at 212.701.3424 or Smarron@cahill.com; MarcAnthony Parrino (associate) at 212.701.3158 or Mparrino@cahill.com; or email publications@cahill.com.