78/79 Consumer Fin. L.Q. Rep. 389

Consumer Finance Law Quarterly Report
2025/2026

Jack Harrington [a1] Christian Hancock [a2] Megan McDowell [a3]

THE EVOLVING FRAUD LANDSCAPE & STRATEGIES TO PROTECT YOUR HELOC CUSTOMERS

*390 I. THE GROWTH OF HOME EQUITY LENDING

Over the past few years, the U.S. consumer finance market has witnessed a striking resurgence in home equity lines of credit (HELOCs)--a form of revolving credit secured by a borrower's home. On average, homeowners now hold approximately $212,000 in tappable equity, with aggregate home equity nationwide estimated at $17.6 trillion. [1] Additionally, according to Intercontinental Exchange (ICE), homeowners took out nearly $25 billion in consumer debt through HELOCs in the first quarter of 2025--the highest first-quarter total since 2008. [2] When combined with cash-out refinances, total equity withdrawals reached $45 billion during that quarter. [3] Despite this uptick, homeowners are currently accessing just 0.41% of the $11.5 trillion in tappable home equity nationwide, suggesting ample runway for continued growth. [4] According to the Mortgage Bankers Association's 2025 Home Equity Lending Study, "total originations of [HELOCs] and closed-end home equity loans increased in 2024 by 7.2 percent from the previous year when comparing originators that reported in both years. Total HELOC and home equity loan debt outstanding grew 10.3 percent." [5] The surveyed lenders anticipated almost 10% growth for HELOC debt in 2025, 7% for home equity loan debt, and further growth in 2026. [6]

Multiple factors have contributed to the renewed popularity of HELOCs. Chief among them is the so-called "lock-in effect": at present, most homeowners hold first mortgages with rates well below current levels, and ***391** there's no incentive to refinance those obligations into higher-rate loans. HELOCs allow these borrowers to retain low-cost loans while accessing relatively inexpensive, flexible credit for renovations, education, or debt consolidation. [7] Although HELOC rates are typically variable, they continue to fall well below those of credit cards and personal loans. At the same time, elevated home values and persistent housing supply constraints have made relocation less attractive. Therefore, more homeowners are choosing to ""improve in place," using HELOCs to fund their remodeling projects and upgrades. [8] Lenders, too, have pivoted toward home equity lending as demand for purchase and refinance mortgages has softened. While traditional depository institutions still originate the majority of HELOCs, their market share has declined from nearly 100% a decade ago to approximately 75% today, as nonbank lenders and fintech platforms entered the space. [9] Investor demand has followed, with a notable increase in the issuance of securities backed by home equity products. [10]

Yet the same features that make HELOCs appealing--on-demand liquidity, minimal borrower interaction post-origination, and remote accessibility--also create vulnerabilities that are increasingly being exploited by fraudsters. From account takeovers to forged draws and identity-based schemes, HELOC fraud is dramatically on the rise. [11] Criminals have learned that a dormant or lightly used HELOC can be commandeered with only a few pieces of personal information, allowing six-figure thefts to occur in a single day--often before the true accountholder even notices. Additionally, HELOC fraud will be closely followed by related litigation against the financial services companies that hold or service the line of credit, as they are often the "last man standing" to whom a consumer may seek recourse.

As HELOC activity continues to climb, so too does the urgency for financial institutions, specifically including mortgage servicers, to adapt their fraud detection and consumer protection strategies. This Article (1) explores the evolving forms of

HELOC fraud and the tactics employed by bad actors, ***392** (2) analyzes the litigation risk and evolving arguments by institutions and borrowers, and (3) presents actionable strategies to strengthen institutional defenses.

To understand how institutions can mitigate these risks, it is first essential to examine how HELOC fraud operates in practice.

II. HOW HELOC FRAUD WORKS

Unlike a purchase-money mortgage, a HELOC can be drawn down multiple times without a full underwriting cycle. That convenience, combined with large available credit limits and less frequent customer oversight, creates three (3) primary attack vectors.

- **Identity Takeover**: criminals assemble personally identifiable information (PII)--date of birth, Social Security number, mother's maiden name--from data breaches, public filings, or dark-web marketplaces. Armed with that data, they submit change-of-address or change-of-contact requests to motor-vehicle agencies and the lender, intercepting mailed statements and authentication codes.

- **Account Manipulation**: fraudsters log in through online or telephone banking, transfer funds from the HELOC into linked deposit accounts, or order official checks payable to shell companies they control.

- **In-branch Extraction**: “Runners” who share the accountholder's ethnicity walk into bank branches with convincingly forged driver's licenses, withdraw cash, and exit before the institution's loss-prevention teams spot anomalies. In sophisticated operations, the proceeds are laundered through casinos, crypto wallets, or third-party money mules, obscuring the audit trail and complicating recovery.

A. Recent Federal Criminal Cases Highlight the Threat.

In May 2025, a federal grand jury in the Eastern District of Pennsylvania indicted three Queens residents (Fanchao Zeng, Zhongzhou Lin, and Yanping Li) on one count of conspiracy to commit bank fraud, five counts of bank fraud, and two counts of aggravated identity theft. [12] According to the indictment, the trio first located customers with sizable HELOCs. Then, they filed fraudulent address changes with the Pennsylvania Department of Transportation and ordered replacement driver's licenses bearing the victims' information but mailed to addresses under the conspirators' control. Using those IDs, they initiated online transfers to intermediary accounts and dispatched runners to bank branches to collect cash or purchase high-value official checks. The group frequently cashed the checks at casinos, disguising the source of funds and muddying Suspicious Activity Report narratives.

***393** Weeks after the Queens indictment, a jury in the Northern District of New York convicted Oluwaseun “Ace G.” Adekoya of bank-fraud conspiracy, money-laundering conspiracy, and nine counts of aggravated identity theft. [13] From a luxury New Jersey apartment, Adekoya harvested homeowner data from commercial marketing files that flag HELOC balances. Via encrypted Telegram chats, he distributed victims' PII, account numbers, and forged driver's licenses to regional “managers” who supervised lower-level impersonators. The conspirators fanned out across the country, impersonated credit-union members at teller lines, and siphoned more than $2 million in HELOC funds. Adekoya laundered his share through nominee bank accounts, luxury jewelry, and a chain of burner phones. Notably, law enforcement tied at least thirteen prior guilty pleas to the same conspiracy, demonstrating how HELOC fraudsters operate as large, disciplined networks rather than isolated bad actors.

B. The Generative AI Accelerator.

While those prosecutions relied on classic identity theft techniques, generative AI is also rapidly weaponizing HELOC fraud. The FBI's December 2024 public-service advisory [14] warned that criminals already use AI in the following ways:

1. Draft flawless phishing emails that evade traditional grammar-based filters;

2. Generate hyper-realistic images for social-media profiles that build trust with potential victims;

3. Clone voices to bypass phone-based identity verification; and,

4. Fabricate high-resolution driver's licenses or utility bills for “know-your-customer” checks.

For HELOC schemes, AI reduces friction at each stage. Image generators erase tell-tale artifacts on counterfeit IDs, allowing runners to pass branch inspection. Large-language models automate scripted call-center prompts, enabling fraudsters to socially engineer changes in contact details without detectable hesitation or linguistic errors. Deep-fake video can even simulate a borrower's face during video-banking authentication. In short, AI collapses the cost curve of deception, letting smaller crews mount nationwide campaigns that were once the province of well-funded criminal syndicates.

*394 C. Why HELOCs Remain Attractive Targets.

Market dynamics reinforce these technological enablers. U.S. homeowners now hold more than $17.6 trillion in tappable equity, and rising interest rates have slowed purchase-money origination, redirecting lender attention and fraud resources toward home-equity products. Bad actors can renew accounts with relative ease because HELOC underwriting often omits title insurance, remote closings are common, and lenders rely on legacy challenge questions easily researched online. The result is an opportunity window in which the creation of the account and unauthorized draws can go unnoticed until the first billing cycle closes, by which time funds may have been irretrievably laundered. Fraud rings also exploit geographic rotation, such as hitting Mid-Atlantic branches one month and Midwest credit unions the next, to stay ahead of pattern-recognition analytics and law enforcement information sharing. Moreover, criminal actors can also fraudulently access legitimately created HELOCs and draw down the lines before a consumer notices.

III. CIVIL LITIGATION RISK MAY BE INEVITABLE

HELOC fraud injures the consumers whose credit lines are fraudulently tapped, and it also raises reputational and litigation risk for lenders and servicers. Mortgage servicers who inadvertently approve fraudulent draws on HELOCs may be sued for violations of the Truth in Lending Act (TILA) and its regulations, the Fair Credit Reporting Act (FCRA), state versions of credit reporting laws, state unfair trade practices laws, state consumer protection laws, breach of the implied duty of good faith and fair dealing, breach of contract, identity theft, negligence, wrongful foreclosure, various versions of the Uniform Commercial Code, and other causes of action. Borrowers have also argued that mortgage servicers were obliged to detect, prevent, or stop fraudulent activity in scenarios where the borrower claims they were being scammed into actively removing funds from their HELOCs. Although the instances of fraud appear to be rising, there are only a few reported cases on point evaluating the legal risk to servicers, and we address a few notable cases herein.

One relevant case arose in 2009, when customers sued their bank after they fell victim to identity theft and an unknown fraudster gained access to their online account and stole $26,500 from their HELOC.[15] The couple alleged violations of TILA, the Electronic Funds Transfer Act (EFTA), the FCRA, Indiana's Uniform Consumer Credit Code, negligence and breach of contract. The court allowed several of the claims to proceed to trial,[16] including claims under the FCRA, TILA, and negligence, finding that *395 whether the bank's security measures were reasonable in the context of a fraud resulting in unauthorized withdrawals was a triable issue of fact.[17] In that case, the plaintiffs alleged that an identity thief accessed their HELOC through the bank's online platform, logging in with their username and password, and withdrew $26,500 without their authorization. They contended that the bank's reliance on “single-factor authentication” (username and password) was insufficient to protect against

such fraud. [18] The plaintiffs further argued that the bank failed to adhere to industry standards, including applicable guidance from the Federal Financial Institutions Examination Council (FFIEC), [19] which recommended multi-factor authentication for high-risk online transactions. [20]

The federal court for the Northern District of Illinois noted that a "number of courts have recognized that fiduciary institutions have a common law duty to protect their members' or customers' confidential information against identity theft." [21] It also found that banks and other institutions "must certainly employ sufficient security measures to protect their customers' online accounts" as part of that duty not to disclose their customers' information. The court then analyzed whether the bank's security protocols met the standard of reasonableness, considering industry best practices and the potential vulnerabilities associated with single-factor authentication. [22] The court determined that because Citizens delayed in complying with the FFIEC security standards (multi-factor authentication), "a reasonable finder of fact could conclude that the bank breached its duty to protect Plaintiffs' account against fraudulent access." **This case illustrates *396 that the reasonableness of security practices--particularly in light of industry standards at the time--is central to determining liability in cases involving unauthorized access.**

In 2011, a California appellate court considered a variety of claims brought against a bank after a fraudster allegedly forged the borrower's signature on two (2) HELOC checks totaling $99,000. [23] The consumer claimed that her bank tried to collect the debt from her, despite her written notice that the checks had been lost or stolen as part of an identity theft and that the bank "failed to diligently investigate [her] notification of identity theft." [24] The consumer asserted that she had never ordered nor received checks for her HELOC and that the defendant bank allowed a third party to access her account and to negotiate the checks. She asserted claims of civil conspiracy, negligence, breach of contract, breach of fiduciary duty, bad faith, breach of the implied covenant of good faith and fair dealing, and violation of California's Business and Professions Code section 17200. The opinion focused largely on the type of account at issue and the statute of limitations, since the consumer had waited more than a year after the alleged theft to file her suit. The earlier dismissal of the borrower's claims was overturned on appeal, opening the door for continued litigation. Although this case is not instructive for the bank's duty to its consumer, it does present a common set of facts for HELOC fraud that any lender or servicer could face under similar circumstances.

In a more recent case from 2024, a borrower asserted that her bank should have saved her from participating in a fraudulent scheme in which she had apparently been caught. [25] Specifically, the borrower had requested and confirmed two five-figure draws from her HELOC in 2020 that totaled nearly $140,000. When the plaintiff requested another $145,000 advance from her HELOC to fund a wire transfer to a third-party account, the bank placed a hold on the account, citing fraud concerns. The plaintiff made multiple requests that the large wire be processed and the defendant responded in writing that it "suspected that the transactions at issue were fraudulent, and further advised that PNC would not process the requested payments unless Plaintiff provided PNC with additional information concerning the legitimacy of these payments." [26] The borrower provided some of the requested information, but PCN still refused to complete the transaction due to its concerns that fraud was occurring. A $285,000 payment to the HELOC account was later reversed by another bank, leaving the HELOC account with a balance of over $290,000.

***397** When PCN declared the account to be in default, the consumer sued, claiming she did not owe repayment of the $140,000 in draws because "she is an elderly woman, and that she was the victim of a scam." [27] She argued that she had fallen prey to a fraudulent scheme. The court summarized her claim as follows:

> As best as the Court can tell, Plaintiff now asserts that, acting at the behest of third parties, including an individual with whom Plaintiff developed a romantic relationship, Plaintiff withdrew large sums of money from the HELOC, and then transferred or attempted to transfer those funds to the third-party fraudsters. **Plaintiff now argues that PNC had a duty to detect, prevent, or stop this fraudulent activity** ... [28]

* * *

> ... [She] now asserts that PNC should have detected the (factually unsupported) third-party fraud at issue and **stopped Plaintiff herself** from conducting authorized transactions that Plaintiff was expressly permitted to make under the terms of the HELOC, i.e., requesting advances under her line of credit following the June 24, 2020,

> $140,000 payment. Essentially, **Plaintiff now asserts that PNC owed Plaintiff a duty to save her from third-party fraudsters who played no direct role, at least with respect to PNC, in the transactions at issue.** [29]

The court rejected the borrower's claim that PCN had breached an implied duty it owed to her. The court noted that, "far from indicating bad faith conduct on PNC's part, the evidence of record tends to establish that PNC acted in good faith in addressing the issues presented herein." [30] The bank servicer intervened after a $140,000 payment was reversed, and it was able to recover a $47,500 wire transfer and return those funds to the checking account. Upon becoming aware of the situation, PNC contacted the customer "to express concern over potential fraud, provided Plaintiff with advice and information about fraud, placed a hold on Plaintiff's bank account, and prevented a further wire transfer of $145,000 to a third-party bank account despite multiple requests from Plaintiff that the transfer be processed." The court repeated that PNC had no express contractual duty to take these actions,

> but doing so certainly undermines any assertion of bad faith conduct on PNC's part. Even if the implied duty of good faith and fair dealing extended so far such that PNC owed a duty to act in good faith in detecting and preventing fraud, no reasonable jury could conclude, on this record, that PNC displayed a lack of diligence such that the duty of good faith and fair dealing was breached in this instance. [31]

***398** The PCN case exemplifies best practices that a lender/servicer can take to prevent fraud, as the bank took several actions to protect the borrower's account, even against her repeated wishes. However, the case also evidences that even such best practices will not prevent litigation when the consumer can only seek recourse with its bank or servicer and not the actual bad actors. Although there is no perfect protection from fraudsters or consumer-litigation, there are warning signs and good practices that lenders and servicers can put in place to protect themselves and their consumers.

IV. ACTIONABLE STRATEGIES FOR LENDERS AND SERVICERS

A. Know the Red Flags and Early Warning Indicators.

Although technology favors the attacker, several red flags routinely surface before a loss event. Fraud investigators should be on the lookout for the following:

- Rapid succession changes in mailing address, email, and phone number;
- Enrollment in paperless statements immediately following a contact change;
- First-time online banking registration for a long-tenured account;
- Bulk ordering of replacement checks or debit cards;
- Large internal transfers from HELOC to deposit accounts followed by outbound wires or cashier's-check purchases; and,
- Same-day branch withdrawals at multiple locations or with multiple tellers.

Positive-pay style controls which require borrower confirmation before advancing funds can frustrate fraudsters, but only if confirmation occurs via an out-of-band channel that relies on previously verified contact data. Importantly, **front-line employees** remain the most reliable early-warning sensor: unexplained nervousness, over-documentation, or scripted answers to seemingly casual questions often precede a fraudulent withdrawal or a fraudulent change to the account that could later impact mailing of HELOC checks. Training tellers or customer service representatives to escalate "gut feelings" without fear of sales-pressure reprisal is therefore an essential control.

B. Operational Controls for Lenders and Servicers.

A layered control environment is the most effective deterrent. At origination, lenders should incorporate biometric or video liveness checks, cross-reference applicant devices against device-reputation databases, and verify title chains to ensure no silent liens exist. During account maintenance, any request to change address, phone, or email should trigger ***399** multi-factor authentication delivered to the original contact channel and a mandatory one-business-day cooling-off period before transactional capabilities are restored. Real-time analytics can score HELOC draw requests based on device geolocation, velocity metrics, and historical customer behavior, placing high-risk requests into manual review queues.

On the servicing side, firms can deploy "positive-pay for HELOCs," emailing or texting accountholders whenever a draw is requested and requiring affirmative confirmation before funds are disbursed. Daily aggregate limits and secondary approval workflows for draws above a defined threshold (for example, $25,000) further restrict loss exposure. Finally, routine penetration tests should include a social-engineering module targeting call-center agents to measure defenses against scripted address-change attempts.

C. Empowering Front-Line Staff and Customers.

Technology alone cannot defeat an adversary that exploits human trust. Mortgage origination companies should embed HELOC fraud modules into onboarding curricula for loan officers, branch managers, and call-center representatives. And servicing companies should do the same for call-center employees. Scenario-based training--showing how a fraudster might layer an address change, online-banking enrollment, and official-check purchase over a seven-day period--helps employees understand the narrative arc of fraud rather than isolated events.

For customers, quarterly fraud-awareness campaigns can remind dormant HELOC borrowers to activate transactional alerts, review statements, and adopt multifactor authentication. Clear, empathetic victim-assistance protocols are equally important. If an account is compromised, the institution should immediately freeze the line, reverse unauthorized draws where possible, provide a dedicated case manager, and supply template dispute letters for credit bureaus. That rapid, transparent response not only mitigates reputational damage but also arms law enforcement with real-time intelligence while the paper trail is still fresh.

D. Partnering with Law Enforcement.

Once fraud is suspected, timing is critical. Mortgage companies should establish pre-existing relationships with the local FBI field office, regional Secret Service electronic-crimes task forces, and state financial-crimes units. Those contacts accelerate subpoenas, video-surveillance requests, and geofence warrants when hours matter. Institutions must also calibrate suspicious-activity reporting to highlight the HELOC angle, using narrative keywords such as "home-equity takeover" or "line-of-credit impersonation," so FinCEN can aggregate filings across multiple banks and spot multi-state patterns.

When a fraud ring is identified, servicers that share detailed loss data, counterfeit IDs, and IP-address logs with law enforcement have historically received favorable consideration in supervisory examinations for their cooperation. ***400** Conversely, institutions that delay notification or treat fraud as a purely civil matter risk regulatory criticism for weak BSA/AML governance and potential consumer-protection exposure if customers suffer cascading credit damage.

V. CONCLUSION

The HELOC industry is up against powerful forces in the evolving nature of identity theft and cybercrimes. Bad actors regularly exploit change-of-address requests, create counterfeit driver's licenses, and use coordinated "runner" networks to steal from unsuspecting homeowners and financial institutions. At the same time, generative artificial intelligence is lowering the cost and raising the sophistication of phishing lures, synthetic IDs, and deep-fake impersonations. For mortgage originators, servicers, and home-equity lenders, the threat environment has shifted from retail-bank nuisance to enterprise-level operational, reputational, and regulatory risk. The industry must remain vigilant and adaptable to the changing risk and can never be complacent with its approach to fraud.

Footnotes

a1 *Jack Harrington is a partner in Bradley's Birmingham, AL office where he leads the firm's Financial Crime & Economic Sanctions team and represents corporations facing complex criminal, regulatory, enforcement, and reputational matters. Prior to joining Bradley, Jack was an Assistant U.S. Attorney with the Department of Justice where he prosecuted complex fraud, money laundering, trade sanctions, cybercrime, and national security matters. Jack received his J.D. from Yale Law School, his M.A. from Georgetown University's School of Foreign Service, and his B.A. from the University of St. Andrews in Scotland.*

a2 *Chrisitan (Chisty) Hancock is a partner in Bradley's Charlotte, NC office and is a practice leader of the firm's Banking & Financial Services group. She is also co-chair of the group's Home Equity Lending sub-team. She specializes in state and federal regulatory compliance for mortgage servicing and origination. She also regularly advises large financial institutions on compliance management systems, government settlements and consent order implementation, bankruptcy-related regulatory matters, and large-scale remediation projects. Christy received her J.D. from the University of North Carolina School of Law and her B.A. (cum laude) from the University of South Carolina Honors College.*

a3 *Megan McDowell is an associate in Bradley's Birmingham AL office and a member of the firm's Banking and Financial Services Practice Group. She advises banks and financial institutions on a wide range of regulatory compliance matters, including mortgage lending, loan servicing, consumer protection, and multi-state licensing. Megan received her J.D. from Cumberland School of Law at Samford University and her B.A. (cum laude) in Economics from Sewanee: The University of the South.*

1 Matt Richardson, *Home Equity Levels Just Hit a New High. Here's Why It's Worth Borrowing Now*, CBS NEWS (June 5, 2025), https://www.cbsnews.com/news/home-equity-levels-just-hit-a-new-high-heres-why-its-worth-borrowing-now/.

2 *ICE Mortgage Monitor: Record Levels of Home Equity and Falling Rates Drive Highest HELOC Withdraws Since 2008*, ICE MORTG. TECH. (June 2, 2025), https://ir.theice.com/press/news-details/2025/ICE-Mortgage-Monitor-Record-Levels-of-Home-Equity-and-Falling-Rates-Drive-Highest-HELOC-Withdraws-Since-2008/; *see also* Andrew Martinez, *Home Equity Lending is Flourishing as HELOC Rates Fall*, NAT'L MORTG. NEWS (June 2, 2025), https://www.nationalmortgagenews.com/news/heloc-rates-fall-and-volume-soars-in-first-quarter-ice.

3 *See ICE Mortgage Monitor: Record Levels of Home Equity and Falling Rates Drive Highest HELOC Withdraws Since 2008*, *supra* note 2.

4 *Id.*

5 *Chart of the Week: HELOC and Home Equity Loan Origination Volume by Known Borrower Usage*, MORTG. BANKERS ASS'N (Aug. 11, 2025), https://newslink.mba.org/servicing-newslink/2025/august/mba-servicing-newslink-tuesday-aug-12-2025/chart-

of-the-week-heloc-and-home-equity-loan-origination-volume-by-known-borrower-usage/?utm_campaign=MBAServicing%20NewsLinkTuesdayAug.122025&utm_medium=email&utm_source=Eloqua.

6 *Id*.

7 HELOCs offer a means of liquidity that preserves the advantageous rates secured during the historically low-rate period of 2020-2021. *See* Jeff Andrews, *Competition for HELOC Business Heats Up as Home Equity Grows*, HOUSINGWIRE (May 20, 2025), https://www.housingwire.com/articles/heloc-originations-increasing-home-equity-mortgage-bankers-association/.

8 Brad Finkelstein, *Home Equity Lending Has Strong Two-Year Runway Ahead*, NAT'L MORTG. NEWS (June 3, 2025), https://www.nationalmortgagenews.com/news/home-equity-lending-has-strong-two-year-runway-ahead.

9 *Id*.

10 Jonalyn Cueto, *Home Equity-Backed Bonds Surge as Borrowing Trends Shift*, MORTG. PROF. AM. (June 6, 2025), https://www.mpamag.com/us/news/general/home-equity-backed-bonds-surge-as-borrowing-trends-shift/538255.

11 Larissa Runkle, *How to Protect Yourself from HELOC Fraud*, BANKRATE (May 29, 2025), https://www.bankrate.com/home-equity/how-to-protect-yourself-from-heloc-fraud.

12 United States v. Zeng, et al., No. 2:25-cr-00225, Dkt. 1 (Indictment) (E.D. Pa. May 21, 2025).

13 *Operation Catch Me if You Can: Elusive Nigerian Ringleader of Nationwide Bank Fraud and Money Laundering Conspiracies Convicted After Two and a Half Week Trial*, U.S. ATT'Y'S OFF.: N. DIST. OF N.Y. (June 26, 2025), https://www.justice.gov/usao-ndny/pr/operation-catch-me-if-you-can-elusive-nigerian-ring-leader-nationwide-bank-fraud-and.

14 *Alert No.:* I-120324-PSA: *Criminals Use Generative Artificial Intelligence to Facilitate Financial Fraud*, FED. BUREAU OF INVESTIGATION (Dec. 3, 2024), https://www.ic3.gov/PSA/2024/PSA241203.

15 Shames-Yeakel v. Citizens Fin. Bank, 677 F. Supp. 2d 994 (N.D. Ill. 2009).

16 The court held the EFTA did not apply to the HELOC account because it is an open-end credit plan of the type explicitly exempted from coverage of the EFTA. *Id*. at 1007 (citing 15 U.S.C. § 1693a(2)).

17 *Id*. at 1008-09.

18 *Id*. at 1000, 1007.

19 *See generally About the FFIEC*, FED. FIN. INST. EXAMINATION COUNCIL (Mar. 17, 2025), http://www.ffiec.gov/about.htm. The "Authentication" document issued by the Council discusses a number of security measures, including tokens, available to banks that offer online banking services. *FFIEC Guidance: Authentication in an Internet Banking Environment*, FED. FIN. INST. EXAMINATION COUNCIL (Oct. 12, 2005) 2, 7-14, https://www.fdic.gov/news/inactive-financial-institution-letters/2005/fil10305.pdf.

20 *Citizens Fin. Bank*, 677 F. Supp. 2d at 1000-01. FFIEC guidance, which applies to both retail and commercial customers, provides:

> The agencies consider single-factor authentication, as the only control mechanism, to be inadequate for high-risk transactions involving access to customer information or the movement of funds to other parties. Financial institutions offering Internet-based products and services to their customers should use effective methods to authenticate the identity of customers using those products and services .... Account fraud and identity theft are frequently the result of single-factor (e.g., ID/password) authentication exploitation.

Citizens Fin. Bank, 677 F. Supp. 2d at 1001.

21 *Id*. at 1008.

22 *Id*. at 1008-09.

23 Fayroyan-Mezhlumyan v. Wells Fargo Bank, N.A., 202 Cal. App. 4th 195 (2011).

24 *Id*. at 826.

25 Feldstein v. PNC Bank, N.A., No. 2:22-CV-01132-RJC, 2024 WL 3430502 (W.D. Pa. July 16, 2024).

26 *Id*. at *2.

27 *Id*. at *3 (emphasis added).

28 *Id*. at *4.

29 *Id*. at *5 (emphasis added).

30 *Id*. at *8.

31 *Id*. at *8.

78/79 CONFLQR 389

End of Document