PEW TRUST WHITE PAPER ON CONSUMER CHECKING ACCOUNTS IS LIKELY TO PROVIDE A TEMPLATE FOR CFPB RULEMAKING

The CFPB is poised to launch rulemakings that will be greatly influenced by a White Paper published by the Pew Charitable Trusts in 2011; it has been updated several times since then. The White Paper is titled “Hidden Risks: The Case for Safe and Transparent Checking Accounts.” The two biggest areas of regulatory concern emerging from the report are (1) automated overdraft programs and (2) the use of arbitration clauses with class-action waivers in deposit account agreements. The White Paper points out that checking accounts are the most prevalent consumer financial product, yet they haven’t gotten the regulatory/legislative attention they need. (The work of the Pew Charitable Trusts in the checking account area can be accessed at www.pewtrusts.org.)

White Paper’s short history of checking account regulation. The White Paper notes that Congress and the regulators have turned their attention to checking accounts on a number of occasions. In 1988, the Expedited Funds Availability Act, implemented by Reg. CC, aided consumers by limiting unreasonable “holds” on deposit accounts. (Comprehensive amendments to Reg. CC have been proposed by the regulators, but have hung in limbo for years.) In 1991, Congress passed the Truth in Savings Act, which was implemented by Reg. DD; the TISA rules have some impact on checking account disclosure, but primarily set forth disclosure standards to help consumers shop for the most attractive rate on certificates of deposit and savings accounts through use of an Annual Percentage Yield. The next legislative step for checking accounts came in 2003, when Congress passed the Check 21 law, which encouraged the scanning of paper checks to speed them through the collection process; as a result, we now have an almost complete digitization of paper check collection, with great improvement in the speed and efficiency of check payments. Ironically, the Check 21 law has helped paper checks continue to be a major payment system.

Since 2009, we’ve seen some other important pieces of consumer protection legislation and regulation in related payment systems. The Credit Card Act of 2009 eliminated a number of abusive credit card practices such as sudden rate increases and unreasonable and disproportional penalty fees. Also in 2009, reflecting a shift in focus from accessing a checking account by check to accessing it by debit card, the Federal Reserve Board amended Reg. E to limit the ability of a financial institution to assess an overdraft fee in a checking account based on paying an ATM or one-time debit card transaction unless the consumer has affirmatively “opted-in” to the overdraft product. At about the same time, the regulators, led by the FDIC, promulgated “guidance” or “best practices” regarding automated overdraft products, including strong discouragement of high-to-low posting of debit card charges.

In 2010, the monumental Dodd-Frank Act gave the CFPB sweeping powers to strike down “abusive” or “unfair and deceptive” acts and practices regarding consumer financial products. This would clearly cover checking accounts.
After five years of operation in which the CFPB did not initiate any rule-making regarding checking accounts, the Bureau now has on its agenda two huge initiatives: (1) outlawing or limiting arbitration clauses with class-action waivers, which nearly every deposit agreement contains and (2) imposing new regulations on overdraft fees and practices. Bankers will be watching these two initiatives very closely. We strongly suspect that the Pew White Paper will have a big influence on the shape of any rule promulgated by the CFPB.

**Major findings of the Pew White Paper regarding checking accounts.** In 2010 the Pew group launched a study of checking account terms and conditions. Pew analyzed more than 250 types of checking accounts offered online by the ten largest banks in the United States; these banks hold nearly 60 percent of all deposit volume nationwide. In researching checking accounts, Pew charted the Median and the range of many checking account fees; the variation in key practices; and the extent of certain practices such as high-to-low debit posting that have been under heavy attack by the regulators and in the courts in the last decade. Based on its research, Pew has identified five checking account practices that “put consumers at financial risk, potentially exposing them to high costs for little benefit.”

*Banks do not provide important policies and fee information in a concise and easy-to-understand format that allows customers to compare account terms and conditions among banks.**

Pew’s research showed that the median length of bank disclosure for key checking account policies and fee information was a whopping 111 pages. “In addition, the banks often used different names for the same fee or service, put the information in different documents, different media (Web or hard copy), or different locations in a document; and did not summarize or collect key information anywhere.” One of the most imaginative proposals is Pew’s Model Disclosure Box for Checking Accounts, which is analogous to the “Schumer Box” for Truth in Lending disclosures. Pew stresses that disclosures are crucial for consumers to make informed decisions, and the information needs to be presented in a format that is clear and understandable.

*Deposit account holders are not provided full information about the respective costs of overdraft options.** All ten of the banks in the Pew study offered “overdraft penalty plans” in which the bank covers overdrafts on an automated basis for a set per-overdraft charge. Nine of the ten banks also offered “overdraft transfer plans” in which an overdraft is shifted to a pre-established line of credit. Another choice is not to enroll in any overdraft plan; the White Paper stresses that this choice avoids fees for ATM and point-of-sale debit card transactions, with rejection of the payment at the ATM or point of sale. Although all these plans have significantly different features and fees, there is no disclosure to facilitate a comparison of costs. Pew concludes that policy makers “should require depository institutions to provide account holders with clear, comprehensive pricing information….”

*Banks overdraft penalty fees are disproportionate to the size of the median overdraft amount.** The iconic example of this practice is that of a $4 cup of coffee at Starbucks that generates an overdraft fee of $35 on the consumer’s debit card. Pew reports that, in 2011, the median overdraft amount was $36 while the median overdraft penalty fee was $35. In addition, the majority of checking accounts charged an extended overdraft fee after a median of seven days if the fees and principal were not paid. The median extended overdraft fee was $25. Under the 2009 Credit Card Act, penalty fees must be “reasonable and proportional” to the size of the violation, and Pew urges that the credit card model be required for overdraft, even though banks contend that overdraft penalty fees are designed to deter use, not to recover costs. Pew concludes that policy makers “should require depository institutions to provide account holders with clear, comprehensive pricing information for all available overdraft options when a customer is considering opting into a program so that the customer can make the best choice among overdraft options—including the option not to incur an overdraft by having the consumer’s bank decline the payment at the ATM or point of sale.

*Strong rejection of high-to-low posting for all payment systems, not just debit cards.** The Pew study categorically rejects use of high-to-low debit posting to maximize overdraft fees. However, it notes that this is one issue where great changes have taken place since its original gathering of data in 2010. Based on FDIC guidance that sharply criticizes high-to-low posting, as well as big-time litigation victories by consumers in class actions in California and Florida, almost all banks have now moved away from the practice, shifting to low-to-high, chronological order, or some variation of these two methods. The Pew study also suggests that the prohibition of high-to-low posting should extend beyond debit card transaction to include overdrafts created by checks and ACH debits.

*The great majority of banks use deposit agreements with mandatory arbitration clauses that include class-action waivers.** The Pew report notes that the Dodd-Frank Act contains a specific provision requiring the CFPB to look closely at consumer arbitration clauses that include class-action waivers. From all indications, the Bureau will prohibit such provisions even though the Pew study doesn’t specifically urge a ban. The upcoming rule-making on this issue is certain to be very contentious and drawn-out. The banking industry will push back strongly against prohibiting class-action waivers, especially in light of the policies behind arbitration found in the Federal Arbitration Act and strong support by recent U.S. Supreme Court decisions, starting with the famous Concepcion case in 2011. The Pew study comes to the
following conclusion on this issue: “The Consumer Financial Protection Bureau, in its study of arbitration agreements, should examine the prevalence of binding arbitration clause; of fee-shifting provisions; and of ‘loss, costs, and expenses’ clauses in checking accounts and assess whether such provisions prevent consumers from obtaining relief.”

**Bottom line.** The Pew study on checking accounts is mandatory reading for bankers because it is already serving as the model for rule-making by the CFPB.

### KEY CONSIDERATIONS FOR FINANCIAL INSTITUTIONS’ CYBERSECURITY PREPAREDNESS

As a result of the recent proliferation of data breaches, cybersecurity is increasingly a top compliance concern for nearly every business. Financial institutions are especially vulnerable, given the amount of sensitive and personal customer data that they maintain. It is, therefore, vitally important that financial institutions take steps to ensure that they have implemented appropriate procedures to help minimize the likelihood that a breach will occur and, if one does occur, to have an appropriate response plan in place. Financial institutions should consider the following in evaluating their risk and determining their cybersecurity preparedness.

**Consideration #1: understand the regulatory landscape.** As data breaches continue to increase in frequency and magnitude, more focus has been placed on developing regulations and legislation to combat the increasing risks. A thorough understanding of the evolving regulatory and legislative landscape related to data security is of key importance for any company’s cybersecurity preparedness. Although cybersecurity legislation is still developing and varies by jurisdiction, a common thread in that legislation relates to notification and information-sharing obligations following a breach. For instance, at least 47 states have laws requiring companies to provide notice to government authorities and/or affected consumers following a breach.

In addition, on December 18, 2015, President Barack Obama signed into law the Cybersecurity Information Sharing Act of 2015, which provides a framework for sharing information between the private sector and government related to cybersecurity threats and breaches. Financial institutions must have a working understanding of these and other relevant data breach laws and regulations to ensure proper preparedness.

**Consideration #2: assess the institution’s risks and develop appropriate policies and procedures.** In order to create an effective cybersecurity program, a financial institution must first assess the risks specific to its particular operations. In making that assessment, it is important to keep in mind that cybersecurity readiness is not a one-size-fits-all proposition. That is, regulators recognize that financial institutions of varying sizes have different risk parameters and should, therefore, have different approaches to cybersecurity preparedness. To that end, the Federal Financial Institutions Examination Council (“FFIEC”) developed a Cybersecurity Assessment Tool, designed “to help institutions identify their risks and determine their cybersecurity maturity.”

The Cybersecurity Assessment Tool provides “a repeatable and measurable process for financial institutions to measure their cybersecurity preparedness over time,” by evaluating the following domains: (1) cyber risk and management and oversight; (2) threat intelligence and collaboration; (3) cybersecurity controls; (4) external dependency management; and (5) cyber incident management and resilience. Financial institutions of all sizes should use the Cybersecurity Assessment Tool to evaluate their risks. In fact, as part of their examinations, many regulators now expect to see proof that financial institutions have used the tool to provide a risk assessment.

Once a financial institution has thoroughly evaluated its cybersecurity risks with the help of FFIEC’s Cybersecurity Assessment Tool, it must develop a plan to manage and minimize those risks. In March 2013, the FFIEC issued a statement “to alert financial institutions to specific risk mitigation related to the threats associated with destructive malware.” That guidance provides the framework for financial institutions to develop their cybersecurity programs. Among other things, the FFIEC guidance encourages financial institutions to take the following steps:

- Securely configure systems and services
- Review, update, and test incident response and business continuity plans
- Conduct ongoing information security risk assessments
- Perform security monitoring, prevention, and risk mitigation
- Protect against unauthorized access
- Implement and test controls around critical systems regularly
- Enhance information security awareness and training programs
- Participate in industry information-sharing forums

It is important to remember that, although the FFIEC guidance provides a comprehensive framework for developing a cybersecurity program, because the technology and methods used by hackers and other bad actors to obtain sensitive data change rapidly, financial institutions must regularly review and update their cybersecurity plans to ensure that those plans account for the latest threats. Further, it is not enough to
simply have written cybersecurity policies and procedures. Rather, efforts must be taken to implement those policies and procedures through regular employee training.

**Consideration #3: vet vendors.** Vendors create a significant risk to financial institutions’ efforts to prevent cyberattacks. That is, vendors often have access to or are in possession of the very data financial institutions seek to protect. Indeed, law firms, product and service add-on partners, payment processors, and others are often entrusted to access or maintain financial institutions’ customer data in the ordinary course of business. However, it is important to remember that just as a chain is only as strong as its weakest link, so too is a cybersecurity plan.

Therefore, financial institutions must ensure that their cybersecurity plans include an evaluation of each vendor’s respective cybersecurity vulnerabilities and preparedness. Those evaluations should include ensuring that vendors have implemented procedures to protect sensitive data, and that those procedures are as thorough in nature as those implemented by the financial institution itself. Simply put, a financial institution’s vendors must be expected to protect sensitive data with the same level of care that the financial institution itself takes to protect the data. Anything less seriously jeopardizes the strength and meaningfulness of the financial institution’s cybersecurity efforts.

Further, financial institutions should evaluate their contracts with vendors to ensure that those contracts require vendors to protect data that they gather, store, disseminate, maintain, or otherwise obtain from the financial institutions. Moreover, financial institutions should consider including provisions that govern liability related to a breach. Because damages related to a breach can flow from various sources, such as reimbursement to affected customers, legal fees, interrupted business expenses, and reputational damage, liability-shifting provisions should be drafted carefully to account for all possible categories of damages.

*Consideration #4: devise and implement a breach response plan. A written data breach response plan is important for a number of reasons. Perhaps the most important reason is to ensure that, in the event of a breach, financial institution personnel understand how to respond in a way that minimizes damage to the financial institution and its customers. In addition, having a written response plan is good evidence during litigation that a financial institution was prudent and acted reasonably.

Although response plans should be tailored to each financial institution, with consideration given to relevant local and federal laws, generally they should include procedures for the following:

- Immediate communication with company personnel regarding a breach and instructions on how to react
- Coordination among members of a designated response team that includes key management and technology personnel, in-house and outside counsel, and the applicable law enforcement agencies
- Steps to identify the cause of a breach and processes to eliminate the source of a breach
- Public relations strategy for notifying the public and affected customers of a breach.

Once a financial institution’s response plan is in place, it is important to simulate a data breach and practice implementing its response plan. A dry run will help key personnel familiarize themselves with the process and ultimately increase the likelihood that the plan will be implemented properly in the event of an actual breach. Further, practicing the response plan will help reveal any deficiencies that may need to be addressed.

**Consideration #5: consider cybersecurity insurance.** Finally, financial institutions should consider acquiring cybersecurity-related insurance. While such insurance obviously increases costs, in the event of a data breach, such insurance can be economically beneficial by helping to offset potentially millions of dollars in costs and damages.

**Bottom line.** Given the increasing risk of data breaches, it is imperative that financial institutions take steps to minimize their vulnerability to such breaches and have proper response plans in place, before a breach occurs. Implementing the tips provided in this article will help to ensure that financial institutions are well on their way to achieving cybersecurity preparedness.

---

**UNIFORM LAW COMMISSION POISED TO PROPOSE MODEL STATUTE ON PROTECTION OF EXEMPTION FOR WAGES DEPOSITED INTO A BANK ACCOUNT**

Both federal and state law provide a number of exemptions from wage garnishment. Most notably, the federal Consumer Credit Protection Act exempts 25 percent of an individual’s earnings from garnishment. 15 USC §1673.
But does this exemption go away when the debtor deposits his or her wages into a bank account? The federal statute is unclear on this point. In something of a surprise, the courts have uniformly held that the exemption does not continue into the deposit account; therefore, the bank is not required to protect the debtor’s exemption when answering a garnishment notice. The leading case is *Usery v. First Nat’l Bank of Arizona*, 586 F.2d 107 (9th Cir. 1978), where the court concluded that the federal statute does not impose a duty on the bank to calculate the amount of the exemption and the applicable number of pay periods. Moreover, the bank is not required to trace the earnings into the account to determine which portion of the deposit is exempt from garnishment.

**Treasury rule regulates garnishment of directly deposited government benefits.** In the name of consumer protection, the federal agencies that disburse benefits, led by the Treasury Department, published an interim final rule in 2011 that requires banks to flag and protect federal benefits, including social security and VA payments, that are exempt from wage garnishment under federal law. The agencies adopted a final rule in 2013. The rule is codified at 12 CFR Part 212. The Federal Register materials accompanying the interim final rule (76 Fed. Reg. 9939-9962) provide a good summary of the compliance requirements imposed on banks:

*A bank that receives a garnishment order must first determine if the United States or a State child support enforcement agency is the plaintiff that obtained the garnishment order. If so, the bank follows its customary procedures for handling the order. If not, the bank must review the account history for the prior two months to determine whether, during this “look-back” period, one or more exempt benefit payments were directly deposited to the account. The bank may rely on the presence of certain ACH identifiers to determine whether a payment is an exempt benefit payment.*

*The bank must allow the account holder to have access to an amount equal to the lesser of the sum of exempt payments directly deposited to the account during the lookback period, or the balance of the account on the date of the account review. This is the “protected amount.”*

*In addition, the bank must notify the account holder that the bank has received a writ of garnishment. The notice must briefly explain what a garnishment is and must include other information regarding the account holder’s rights. There is no requirement to send a notice if the balance in the account is zero or negative on the date of account review. Banks may choose to use a model notice contained in the rule in order to be deemed to be in compliance with the notice requirement.*

*For a deposit account containing a protected amount, the bank may not collect a garnishment fee from the protected amount. The bank may only charge a garnishment fee against funds in the account in excess of the protected amount and may not charge or collect a garnishment fee after the date of account review.*

*Banks that comply with the rule’s requirements are protected from liability.*

Banks have now lived with these compliance requirements for five years, while consumers have enjoyed protection of the exemption where federal benefits are involved.

**ULC proposes uniform wage garnishment legislation that builds upon the Treasury rule model.** In July of 2016, the Uniform Law Commission will take a final vote on promulgation of a uniform Wage Garnishment Act. Article I of that proposed legislation deals with garnishment of earnings generally, with emphasis on the relationship between the garnishing creditor (garnisher) and the employer (garnishee). Article I establishes a legal framework for (1) the commencement of a garnishment action; (2) the initial response of the garnishee to the garnishment action; (3) the pendency of a garnishment; (4) termination of a garnishment action; (5) notice forms; (6) limits on wage garnishment; (7) multiple ordered deductions; (8) compliance process; and (9) garnishee penalties for noncompliance. The goal of the drafter’s is to bring some uniformity to this area of state law.

Article II of the proposed legislation deals with garnishment of bank accounts titled in the name of an individual that contain exempt earnings. These provisions build upon the Treasury rule dealing with the garnishment of bank accounts containing federal benefits. This should simplify bank compliance. Set forth below is a summary of Article II by William Henning, Professor of Law at Texas A&M School of law. Professor Henning chairs the Drafting Committee for the proposed legislation. Here is his nutshell:

*Article II includes the requirement that a bank conduct an account review with a 60-day lookback period within two days after being served with a garnishment order—the same as under the Treasury rule. In conducting the review, the first step is for the bank to determine whether there were two or more direct deposits from the same source during the lookback period. The bank doesn’t have to determine whether the deposits were from an employer; if there are not two direct deposits from the same source, the act doesn’t permit the account holder an exemption and the bank’s responsibilities under the act are at an end.*

*If there are two direct deposits from the same source during the lookback period, the bank must send a notice to the account holder not later than three business days after the account review, just as under the Treasury rule. If federal benefits were deposited during the lookback period, the bank can use the federally mandated form, amended to
include a very limited amount of additional information—a statement that the account holder can claim an exemption, the beginning date of the lookback period, and an explanation of the process for claiming the exemption.

If there are no federal benefits in the account, the bank must send a form that mirrors the federal form, except for the addition of the same limited amount of information described above. The act contains a standard form for providing the additional information that will make compliance easy.

*Once the bank sends the notice, it waits to see if the account holder claims an exemption. If it does not receive a form claiming an exemption within 15 days after the date on the notice to the account holder, its duties under the act are at an end. The form the account holder is to use is provided in the notice sent by the bank. Even if the account holder claims an exemption, the bank’s duties under the act are at an end if it does not receive one or more pay stubs from the account holder within 15 days after it received the account holder’s claim form.

*If the bank receives pay stubs, it reviews them to see if the earnings were direct-deposited to the account at issue and if the date of payment is within the lookback period. If the answer to those questions is yes, the bank looks to see whether the pay stubs indicate an amount that was garnished. The total amount of garnished funds shown on qualifying pay stubs is the amount of the exemption. The bank’s good-faith determination of the exempt amount is conclusive and not subject to challenge by the creditor or the account holder.

Some final thoughts:

*The drafters of the proposed legislation summarize their efforts dealing with garnishment of bank accounts: “We have structured [Article 2] to be closely aligned with our primary mission, which is regulation of garnishment by employers. As a result, the exemption only applies if the account contains earnings that have already been subjected to some type of prior garnishment within the lookback period, including garnishments governed by Article 1 [dealing with garnishment of employers]. Similarly, the amount protected in [Article 2] is closely tied to those earnings.”

*The drafters also point out that, at the present time, 35 states provide some type of protection for bank depositors against garnishment, but the nature and scope of the protection varies considerably among states. The proposed legislation would bring uniformity and predictability to this area of the law.

*If the proposed garnishment legislation is to be widely adopted by the states, it will require the support of the two key constituencies: consumers and banks. We think that the proposed legislation does a good job of protecting the exemption of consumers from garnishment after the wages are deposited into a bank, while at the same time seeking to ease the compliance burden of the banks. The legislation deserves careful attention by the states.

*It is possible that the ULC will end up proposing only Article I, dealing with situations where the employer is the garnishee, rather than including Article II, where the bank is garnishee. We think the best approach is to combine the two Articles in the proposed legislation and let the individual states decide whether to delete Article II.

IN CASE INVOLVING FRAUDULENT DUPLICATE REAL ESTATE NOTES, FLORIDA COURT RESOLVES PRIORITY DISPUTE BASED ON ARTICLE 9 RULES

In a notable decision from Florida, the court ruled that, as between two mortgage assignees, priority goes to the first assignee to perfect its security interest in one of two duplicate notes secured by the mortgage. The guiding principle is that “the mortgage follows the note.” The decision seems correct.

The Florida duplicate-note case. In HSBC Bank USA, N.A. v. Perez, 165 So. 3d 969, 86 UCC Rep. 2d 565 (Fla. Dist. Ct. App. 2015), the borrower unwittingly executed two nearly identical promissory notes at a mortgage closing. The notes were payable to the same secured lender, for the same amount, and secured by the same mortgage. The execution of the duplicate notes was part of a larger fraudulent scheme that included other loans. The first assignee (HSBC) closed on a pooling and servicing agreement (PSA) with the lender and took possession of one of the borrower’s two “original” notes. Later, another assignee (LaSalle) entered into a separate PSA with the lender, which led to its taking possession of the borrower’s second “original” note. The court ruled that, by taking possession of its note first, the first assignee had priority over the second and was thus entitled to foreclose. It didn’t matter whether the assignees had recorded any assignments of the underlying mortgages.

In reaching this result, the Florida court turned to Article 9 of the UCC. Article 9 does not “apply to the creation of a real property mortgage” UCC 9-109(a)(11). However, if the note in a mortgage transaction is sold or assigned as collateral, Article 9 applies to the security interest created in favor of the purchaser or assignee of the note. Comment 7 to 9-109 gives an example:

O borrows $10,000 from M and secures its repayment obligation, evidenced by a promissory note, by granting to
M a mortgage on O’s land. [Article 9] does not apply to the creation of the real-property mortgage. However, if M sells the promissory note to X or gives a security interest in the note to secure M’s own obligation to X, [Article 9] applies to the security interest thereby created in favor of X. The security interest in the promissory note is covered by [Article 9] even though the note is secured by a real-property mortgage.

Attachment, perfection and priority. Under UCC 9-203, HSBC’s security interest attached, at the latest, when it took possession of the note. Similarly, under 9-313, its security interest in the note was perfected when it took possession. Both the timing and the method of perfection are crucial to establishing priority. The key Article 9 rule is found at 9-322, which provides that conflicting perfected security interests “rank according to priority in time of filing or perfection.” When neither party perfects by filing (as in the present case), the rule is first-to-perfect. By taking possession of its promissory note before LaSalle took possession of its note, HSBC was the first to perfect its interest in a note connected to the underlying mortgage. Therefore, HSBC had priority to the note and, derivatively, to the mortgage.

The Florida court relied heavily on a leading New York case involving almost identical facts, Provident Bank v. Community Home Mortgage Corp., 498 F. Supp. 2d 558, 63 UCC Rep. 2d 155 (E.D.N.Y. 2007). In that case, the defendant, a mortgage warehouse lender, engaged in a scheme known as “double-booking,” where mortgage borrowers unknowingly executed duplicate original notes and mortgage assignments in order to obtain duplicate funding for one loan from two different sources. Under this scheme, the fraudster sold nine promissory notes to two banks—NetBank and Southwest Securities Bank. In most of these cases, Southwest recorded its mortgage assignments first in the real estate records, but NetBank was the first to take possession of the notes. Southwest contended that it had priority based on its real estate recording, while NetBank argued that it had priority based on the first-to-perfect rule governing the promissory notes. The court gave priority to NetBank under Article 9 and the principle that “the mortgage follows the note.” Article 9 filing trumps real estate recording. The Florida court concluded that applying the UCC rules makes sense, even though Article 9 was not really designed to deal with transactions involving duplicate notes.

Variation on the duplicate note scam. Anecdotally, we have heard of closely related scams that don’t employ duplicate notes, and rely more on negotiable instruments law than Article 9, but still depend on the proposition that “the mortgage follows the note.”

Example: Home Equity Corp. originates a portfolio of high-interest second-mortgage home equity loans. Each loan is evidenced by a negotiable promissory note and a second mortgage. In turn, Home Equity grants a security interest in the loans to First National Bank as collateral for a line of credit. Each note is endorsed and delivered by Home Equity to the bank. The bank does not record any assignments of the mortgazes in the real estate records. The bank allows the homeowners to continue making their monthly payments to Home Equity. However, when Home Equity falls into default on its loan, the bank notifies the obligors to begin making payments directly to it.

At that point, the bank discovers that Home Equity had fraudulently purported to “sell” the loans to investors by executing “assignments” of each loan and recording those assignments in the real estate records. The investors were unsophisticated. They assumed that they had full ownership of the loans based on the recorded assignments, even though they made no attempt to obtain possession of the notes. Aware of the competing claims to the loans, the bank brings a declaratory judgment action to determine priority. At the time of the loan, the bank had no idea of the competing claims and never checked the real estate records. In the wake of these revelations, Home Equity files bankruptcy.

In this example, who has priority to the mortgage loans? Under general principles of law and tenets of public policy, the bank should have priority. The notes are negotiable instruments. They would be treated as such by participants in the secondary market or by lenders relying on them as collateral. Parties to secondary market transactions know or should know that the promissory note is the key document in any mortgage loan transaction. The mortgage itself, although it enhances the value of the note as a monetary obligation, is always ancillary to the note. Therefore, the party who qualifies as a holder in due course of the note also locks up priority to the mortgage that secures the note.

A related principle is that a recorded “assignment” of the mortgage is a nullity if the assignee fails to obtain possession and endorsement of the note itself (or on an allonge). That is exactly what happened in the example. Because the unsophisticate investors relied on recorded “assignments” of the mortgazes by the fraudulent originator without the notes themselves, they never had good title to the loans. In short, the bank should have priority to both the notes and the real estate mortgages, as well as standing to foreclose.
These legal rules promote sound public policy. Participants in the secondary market, and banks making loans against real estate notes, must be able to rely on their status as holders in due course of negotiable instruments, with power to take the instruments free of any adverse claim. Without this assurance, the markets would be in a state of constant uncertainty. Specious claims based on bogus “assignments” recorded by fraudulent loan originators would seriously undercut the liquidity of mortgage loans. Taking possession of the promissory note as a holder in due course is the gold standard of marketability of the loan that is evidenced by the instrument. Conditioning the bank’s priority on making it do a real estate search before it takes a pledge of the notes would compromise their transferability. 

**Bottom line.** Both Article 3 (codifying the law of negotiable instruments) and Article 9 (codifying the law of secured transactions) have an important role to play in disputes regarding the assignment of real estate mortgage loans.