March 2021

How Fintech is *Changing* Vendor Management

special report

Sponsored by:

Qualia

Produced by:

Dodd Frank
UPDATE

ABOUT US

Contact information:
October Research, LLC
ATTN: Valuation Review
3046 Brecksville Road, Suite D
Richfield, OH 44286
Tel: (330) 659-6101
Fax: (330) 659-6102
Email: contactus@octoberresearch.com

EDITOR'S NOTE

ALWAYS LEARNING, ALWAYS GROWING

Dear Readers,

One of my favorite things about doing a report on a new topic is the opportunity to learn about a specific niche in our industry. In this report on fintech and vendor management, we dive into an interesting, less discussed topic for our publication.

From a regulatory review to speaking with **Michael Steer** of Mortgage Quality Management and Research, LLC to sleuthing out tips and recommendations for vendor-lender relationships, *Dodd Frank Update* gathered valuable information we now hope will benefit you as the industry continues to grow and evolve, largely with the support of fintech companies and other third-party service providers.

One of my biggest takeaways from the knowledge inside this report is communication is key to any relationship, especially professional ones. Many of the recommendations we found highlighted the need for a clear service agreement with set boundaries, and consistent contact between third-party service providers and lenders to maintain a compliant and beneficial partnership.

Lastly, we would like to thank Qualia for sponsoring this report so we could make it available as a free resource for professionals.

Stay in touch (but socially distant),

Elizabeth C. Childers, Esq.

Elizabeth C. Childers, Esq.
Editor
echilders@octoberresearch.com

Dodd Frank UPDATE
OCTOBER RESEARCH LLC

CONTENTS

Regulatory requirements for vendor management

Before delving into the nitty gritty, let us review what the regulatory agencies say about using third-party providers (also referred to as service providers or vendors) in the mortgage and banking industries.

The Consumer Financial Protection Bureau (CFPB) is not the only entity to regulate these relationships. The Office of the Comptroller of the Currency (OCC), the Federal Deposit Insurance Corp. (FDIC), and the National Credit Union Administration (NCUA) have all issued guidance on managing third-party providers and the regulatory compliance involved.

CFPB

Section 1002(26) of the Dodd-Frank Act defines a service provider as "any person that provides a material service to a covered person in connection with the offering or provision by such covered person of a consumer financial product or service."

The CFPB allows for supervised banks and nonbanks to outsource certain functions to service providers.

The bureau recognizes there are several reasons why using a third party would be an appropriate business decision for supervised banks and nonbanks, such as resource constraints, the availability of expertise not otherwise available without significant investment, and the opportunity to develop and market additional products or services.

However, the bureau warns supervised entities there are risks involved when using a third-party provider.

"A service provider that is unfamiliar with the legal requirements applicable to the products or services being offered, or that does not make efforts to implement those requirements carefully and effectively, or that exhibits weak internal controls, can harm consumers and create potential liabilities for both the service provider and the entity with which it has a business relationship," the CFPB stated in its guidance. "Depending on the circumstances, legal responsibility may lie with the supervised bank or nonbank as well as with the supervised service provider."

The same regulation that authorizes the CFPB to examine and obtain reports from supervised entities also grants it the authority to do so for supervised service providers and their on-site operations. As a result, the bureau expects supervised banks and nonbanks alike to have processes to manage risks associated with third-party providers.

The bureau's expectations for risk management programs are commensurate with the size, scope, complexity, importance, and potential for consumer harm associated with the relationship. The type of service and the performance in carrying out such activities also is considered when the bureau determines whether a supervised entity's program achieves due diligence.

"While due diligence does not provide a shield against liability for actions by the service provider, it could help reduce the risk that the service provider will commit violations for which the supervised bank or nonbank may be liable," the bureau stated.

Though these are only suggestions, and other steps may be necessary depending on the vendor relationship, the CFPB recommends:

- "Conducting thorough due diligence to verify that the service provider understands and is capable of complying with Federal consumer financial law;
- Requesting and reviewing the service provider's policies, procedures, internal controls, and training materials to ensure the service provider conducts appropriate training and oversight of employees or agents that have consumer contact or compliance responsibilities;
- Including in the contract with the service provider clear expectations about compliance, as well as appropriate and enforceable consequences for violating any compliance-related responsibilities, including engaging in unfair, deceptive, or abusive acts or practices;
- Establishing internal controls and on-going monitoring to determine whether the service provider is complying with federal consumer financial law; and
- Taking prompt action to address fully any problems identified through the monitoring process, including terminating the relationship where appropriate."

OCC

"The [OCC] expects a bank to practice effective risk management regardless of whether the bank performs the activity internally or through a third party," the agency stated. "A bank's use of third parties does not diminish the responsibility of its board of directors and senior management to ensure that the activity is performed in a safe-and-sound manner and in compliance with applicable laws."

The agency stated it was concerned the quality of risk management programs are not keeping pace with the level of risk and complexity of these relationships. In its supervision, it has observed national banks and federal savings associations fail to properly assess and understand the risks and direct and indirect costs involved with service providers; fail to perform adequate due diligence and ongoing monitoring of those relationships; entering into contracts without evaluating the third party's risk management practices; and even engaging with service providers without executing a contract.

Like the CFPB, the OCC suggests those under its jurisdiction develop a risk management process commensurate with the level of risk and complexity of its third-party relationships. Its recommended process includes plans that outline the bank's strategy; identification of the inherent risks of the activity, and details how the bank selects, assesses, and oversees the third party; proper due diligence in selecting a third party; and written contracts that outline the rights and responsibilities of all parties.

The OCC also recommends these plans take into account the "ongoing monitoring of the third party's activities and performance; contingency plans for terminating the relationship in an effective manner; clear roles and responsibilities for overseeing and managing the relationship and risk management process; documentation and reporting that facilitates oversight, accountability, monitoring, and risk management; and independent reviews that allow bank management to determine that the bank's process aligns with its strategy and effectively manages risks."

FDIC and NCUA

The FDIC has similar guidance as the OCC and the CFPB, breaking down its recommended risk management process into four elements: risk assessment, due diligence in selecting a third party, contract structuring and review, and oversight.

"The FDIC reviews a financial institution's risk management program and the overall effect of its third-party relationships as a component of its normal examination process," the agency stated. "As noted, the FDIC evaluates activities conducted through third-party relationships as though the activities were performed by the institution itself. In that regard, it must be noted that while an institution may properly seek to mitigate the risks of third-party relationships through the use of indemnity agreements with third parties, such agreements do not insulate the institution from its ultimate responsibility to conduct banking and related activities in a safe and sound manner and in compliance with law."

In addition to these recommendations, the FDIC also specifically reminded financial institutions under its jurisdiction to comply with Section 7 of The Bank Service Company Act, which requires insured financial institutions to notify their appropriate federal banking agency in writing of contracts or relationships with third parties that provide certain services, such as check and deposit sorting and posting.

The NCUA also provides significant guidance and suggestions for federally insured credit unions. In its supervisory letters, the agency gives entities a standard framework for reviewing third-party relationships. The guidance contains a lot of the same steps, with the same emphasis that each vendor should be assessed for compliance on a case-by-case basis.

"This guidance was developed to assist in the evaluation of basic planning, due diligence, and controls credit unions should have in place when engaging in third-party relationships," former NCUA Chairman **JoAnn Johnson** wrote in a letter to boards of directors. "The planning, due diligence, and controls required to safely engage in these relationships will depend upon credit union risk profiles and the type of relationship with the vendor."

> "The planning, due diligence, and controls required to safely engage in these relationships will depend upon credit union risk profiles and the type of relationship with the vendor."
>
> **JoAnn Johnson**, former chairman, NCUA

With all of these regulations to keep in mind, and the time it takes to maintain these relationships and ensure compliance, it is no wonder companies are looking for assistance. This is where financial technology (fintech) companies like HQ Vendor Management (HQVM) have stepped in over the years.

"HQ Vendor Management is a dba of Mortgage Quality Management and Research, LLC (MQMR)," MQMR President **Michael Steer** told *Dodd Frank Update*. "MQMR founded HQVM in 2014 to deliver an all-inclusive, cost-effective and customizable vendor management solution to meet third-party oversight requirements.

"HQVM's mission is to strategically manage vendors to maximize an organization's investment in outsourcing," he continued.

"As a mortgage services firm built by mortgage bankers for mortgage bankers, HQVM combines expertise and technology to deliver comprehensive vendor management solutions that suit each lender's unique operational requirements and risk tolerance.

"As one of the few vendor management firms specializing in the mortgage industry, HQVM is equipped to handle key aspects of mortgage vendor oversight, including vendor assessments, due diligence questionnaire development, vendor risk analysis, on-site vendor reviews and reporting for compliance purposes. HQVM's experienced team includes credit analysts, financial analysts, attorneys and auditors whose collective skills and expertise establish a unique platform to audit vendors and assess risk."

How COVID-19 has impacted vendor management

It is no longer news that COVID-19 continues to have a huge impact on the mortgage industry. With low interest rates and high consumer demand, many mortgage businesses and banks had record years in 2020 while many other industries struggled.

It also is no secret that with the issues brought on by the pandemic, financial technology (fintech) companies have had the opportunity to step up their game and assist the industry in its sudden need to join the digital age.

HQ Vendor Management (HQVM), a dba of Mortgage Quality Management and Research, LLC (MQMR) is one of those companies.

"While our business faced many of the same general business challenges as everyone else — the transition to remote work, no travel, more workday interruptions, etc. — the near-total ban on vendor on-site audits meant that we had to get creative not only in conducting our reviews, but also in preparing our clients for remote regulatory exams," MQMR President **Michael Steer** said.

"From the client perspective, we observed that lenders were more willing to onboard vendors that could help them address the immediate challenges facing their organizations, primarily the tremendous increase in volume as well as technologies that provided more remote or digital capabilities. Most lenders were making decisions between 'need-to-have' technology and services versus the 'nice-to-have,' even when the 'nice-to-have' would potentially benefit their business in the long term.

"Lenders also began looking at offshoring to solve for the shortage of talent in the face of astronomical volumes, with a focus on process efficiency and outsourcing highly manual tasks to enable domestic staff to focus on their core job responsibilities."

Steer said the biggest concerns among HQVM's clients are information technology (IT) and cybersecurity for their own operations and those of their vendors.

"What's interesting is that many industry vendors had already established fairly stringent data and cybersecurity protocols because of the varying requirements of all the lenders with whom they work, whereas some of the lenders we audited still have some holes in their protocols, such as having USB access on company machines," Steer said. "This is very risky because it allows someone to download potentially sensitive data at will, and it's pretty shocking to see in today's environment.

"In addition, we've seen that some of the offshore vendors our clients are working with have even better security protocols than their domestic counterparts, including biometrics, 24/7 security guards and requiring employees to check their personal electronics at the door," he added.

Steer said his company recommends clients who are engaging in remote work establish the ability to shut down data downloads outside of their network; block employees from accessing certain websites when on the company network and/or device; and reinforce using in-office security protocols when teleworking, such as locking computers when not in use.

What fintechs can do to help with vendor management

Lenders who don't outsource their vendor management needs often rely on spreadsheets, calendar reminders, and email to keep up with third-party providers.

Michael Steer, president of Mortgage Quality Management and Research, LLC (MQMR), said this results in a fragmented and inefficient process. MQMR owns HQ Vendor Management (HQVM), a financial technology (fintech) company specializing in managing third-party providers for businesses in the mortgage industry.

Steer said companies seeking HQVM's services say their biggest challenges when it comes to vendor management are a lack of internal resources and subject matter experts. Smaller lenders may only have one person who handles vendors, and it might not be their only role in the organization.

"Furthermore, finding someone with both the depth and breadth of experience necessary to assess all aspects of a vendor's operations is a tall order that not every lender can fill," he said. "As a result, vendor management responsibilities are often spread out across multiple functions and departments within the lender's organization, which can create confusion and uncertainty in the process — not to mention being just plain inefficient. Then, there is the added concern of key person dependency. If the one person overseeing vendor management leaves or is out for an extended period, who picks up those responsibilities in his or her absence?

"At its core, vendor management is a manufacturing process, and having specific people reviewing specific parts of the process (contracts, financials, cybersecurity, etc.) ensures that lenders walk away with a clear and comprehensive picture of the nature of the vendors with whom they are contracted and the unique level of risk each and every vendor poses to their organization."

HQRM and other companies like VendorRisk and Venminder offer solutions to the inefficiencies that can plague internal vendor management.

"Quite simply, fintech vendor management software allows lenders to do more with less," Steer told *Dodd Frank Update*. "By using software specifically tailored for oversight of vendors, lenders can centralize both their documentation and the review processes, which provides more visibility into the full scope of their vendor network and enables them to dig deeper to gain a better understanding of each vendor.

"Many of these platforms also include the ability to incorporate a scoring methodology that allows lenders to rate the overall risk each vendor poses to their organization based on certain criteria. Recreating this functionality using a spreadsheet is a daunting endeavor."

VendorRisk is a software as a service (SaaS) product that is a web-hosted application developed, maintained, and hosted by the company. On its site, the organization states its software stores all vendor information in one place, making it easier to manage contacts and agreements. Companies can choose the features they need, from due diligence questionnaires to incident tracking to risk reviews.

HQVM, along with several other companies, partners with VendorRisk to offer services such as designing risk and diligence questionnaires; assisting in vendor and contract data collection; reviewing and identifying any vendor issues and creating a resolution plan; conducting diligence on vendors; providing updated risk questionnaires as regulations change; ongoing review of industry and regulatory websites to remain current and compliant; and/or proactively communicating findings to internal and external auditors.

Venminder is another vendor risk management company that offers a variety of solutions, from SaaS to vendor risk assessments to managed services. According to its site, its experts complete 30,000 vendor risk assessments annually and 900 organizations use its products or services to mitigate vendor risks. Venminder services several different industries, including financial services, insurance, and real estate.

Steer said vendors also benefit from fintech vendor management solutions.

"From a vendor standpoint, these automated platforms often leverage skip logic in their vendor due diligence questionnaires, which creates a better vendor experience by allowing them to bypass questions that do not apply to their organization," Steer said. "As a result, vendors are more willing to complete these questionnaires, which form a key component of the ongoing vendor oversight process. In addition, lenders have the ability to create vendor questionnaires very quickly and track their status using an automated system."

Steer said one of the biggest benefits to using a fintech company to manage third party providers is their ability to learn the industry's best practices.

"These systems are designed to be used by a wide variety of lenders and leveraging the collective knowledge of multiple organizations on addressing vendor risk creates a significant advantage to using a vendor management platform," he said.

"In addition, there is a lot to be said for the time and money lenders save by utilizing a solution created specifically to conduct vendor management. Customizing more general software to meet this specific need requires a significant investment in time and financial resources, and even if an organization is willing to commit both of these to this endeavor, there is still the risk that the resulting system may not meet all of the organization's needs."

"There is a lot to be said for the time and money lenders save by utilizing a solution created specifically to conduct vendor management."

Michael Steer,
president,
Mortgage Quality Management and Research, LLC (MQMR),

Fintech tips for vendor relationships

Managing vendor relationships end-to-end can be tricky business. But it doesn't have to be. **Michael Steer**, president of Mortgage Quality Management and Research, LLC (MQMR), offered some guidance for those in the mortgage industry that are unsure about what they should be doing to properly manage their third-party provider relationships.

"Before vetting a new or existing vendor, the first question lenders need to answer is, 'What are the objectives or outcomes of the due diligence process?' " Steer said. "From there, lenders need to assess the maturation of their vendor management program to determine what elements they have in place and where there may be gaps."

Steer said one of the biggest challenges for lenders is having a complete understanding of every vendor connected to their organization. Even a vendor that is not directly related to the loan origination and/or service process could potentially open a company up to liability. Knowing the full list of their company's vendors is critical, he said.

"Lenders also need to understand that there is more to vendor management than simply reviewing their vendors," Steer added. "This function also includes vendor search and onboarding, in addition to on-going reviews and monitoring. For many lenders, vendor management tends to focus primarily on the beginning and secondarily on the middle of the vendor relationship, but most often, lenders fail to account for the end by overseeing the deboarding process when a vendor relationship ends.

"Then, of course, there are the regulatory considerations. Vendor management is required by a host of regulators, and generally speaking, a lender's vendor management program needs to be able to provide satisfactory answers to the following questions:

- "Who are your vendors?
- What does each contracted vendor do for your company?
- What kind of access do they have to your data?
- Who do they touch in the course of their activities on behalf of your company (borrowers, real estate agents, underwriters, etc.)?
- Who is the vendor as a company from an operational, financial and reputational standpoint?
- What level of risk does each contracted vendor pose to your company?"

The Federal Deposit Insurance Corp.'s (FDIC) guidance on third-party providers also offers a list of items a lender should consider when vetting a potential vendor.

"Comprehensive due diligence involves a review of all available information about a potential third party, focusing on the entity's financial condition, its specific relevant experience, its knowledge of applicable laws and regulations, its reputation, and the scope and effectiveness of its operations and controls," the FDIC stated.

When evaluating a third party, a lender should ask for or consider at least some of the following: audited financial statements, annual reports, filings with the U.S. Securities and Exchange Commission; the significance of the proposed contract to the vendor's financial condition; the vendor's business reputation and qualifications; business resumption strategy and contingency plans; and knowledge of relevant consumer protection and civil rights laws and regulations.

Many potential uncertainties that can arise in a vendor-lender relationship can be resolved by starting with a comprehensive service agreement. A fully executed and well thought out contract can create clearly defined expectations and processes for initializing the service, managing audits and reviews throughout the relationship, and how the parties will conclude business in a way that protects both from liability.

HQ Vendor Management (HQVM), a dba of MQMR, offers advice as to what contract provisions should be included to ensure a healthy and compliant vendor relationship.

"Contracts that clearly define vendor responsibilities restrict lender liability, strengthen contract enforceability and give lenders greater leverage in addressing service violations and performance related disputes," the company stated.

HQVM suggested vendor agreements should contain information such as the nature of the services provided, the expected standards of service performance, the frequency with which services will be performed, and the effective length of service duration. It is important to set service boundaries, the company stated, because protections may not cover activities outside the scope of the agreement.

Other recommended contract provisions include confidentiality provisions for transmitted data and trade secrets; a clear understanding of the vendor's security breach protocol; agreeable termination provisions, or renewal dates; verification of adequate insurance coverage; guarantees the lender has the right to audit or monitor the vendor; assignment provisions with clear stipulations; indemnification clauses that outline what circumstances the lender would be required to indemnify the vendor; dispute resolution procedures; non-compete and non-solicitation provisions; provisions for offshore services; compliant record retention policy; and a clear process to give the lender access to their information once the relationship is terminated.

As to what the oversight of third-party vendors should look like, the FDIC stated what is considered appropriate monitoring depends on the type of vendor and the type of relationship.

In general, lenders should regularly review the overall effectiveness of the vendor relationship and whether it is consistent with the lender's goals; any licensing or registrations to ensure the vendor can legally perform its services; the vendor's financial condition, on at least an annual basis; and how well the vendor is adhering to and maintaining the requirements listed in the service agreement.

The agency also recommended regular meetings between the vendor and lender representative to discuss any performance or operational issue as they come to light.

Fintech products revolutionizing the lending industry

Whether it is identifying fraud or ensuring compliance with various state and federal laws, fintech companies are vital to banks and lenders.

In addition to helping navigate fraud and compliance, fintech companies supply the tools that are helping banks and lenders modernize infrastructure and product delivery, upgrade banking stacks, and even efficiently process Paycheck Protection Program (PPP) loans.

Recent examples include:

First Horizon recently selected Finxact to underpin its product and service delivery through its VirtualBank brand. First Horizon, which merged with Iberiabank in 2020, has $84 billion in assets, $60 billion in deposits, and services over one million customers spanning 11 states.

First Horizon said by using their VirtualBank brand as an innovation ground for long term technology modernization, it will deliver technology capabilities that compete with all-comers in the marketplace while maintaining a focus on their existing client base.

"VirtualBank's conversion to the Finxact cloud core is an important step in First Horizon's overall efforts to modernize infrastructure and product delivery," First Horizon Chief Operating Officer **Anthony Restel** said. "This is an opportunity to test and learn the most efficient and effective ways to serve our clients in the future."

Finxact said its platform includes a comprehensive and extensible financial services model exposed as APIs (application programming interface). By accessing its open APIs and extensible components, Finxact said banks can invent, curate, and launch products at the speed required to meet customer expectations in today's marketplace.

"We are honored that the First Horizon team found in Finxact a platform that meets their demands for the level of performance, scale, and resiliency required for the next generation of banking," Finxact founder and CEO **Frank Sanchez** said. "Our solution is uniquely suited for an institution of their size and ambitions."

Finxact secured a $30 million strategic investment from banking and financial services firms in 2019 and is currently working with multiple U.S. and international financial institutions, from de novo banks to top-tier banks, on projects ranging from full core conversions to digital-only initiatives.

Berkshire Bank recently selected Cirrus' document collection portal to help the bank manage an influx of SBA loan requests, including 942 PPP loans on the first day of the program.

Berkshire said Cirrus will help it eliminate the inefficiencies and delays that often hinder overall accuracy, workload, and response times. Cirrus said its cloud-based system supports collaboration throughout the entire loan process by streamlining document management, ensuring Berkshire Bank and its customers have real-time status updates into the progress of each loan.

Berkshire said automating the collection and collaboration of loan documents allows it to better manage extensive loan requests and provide quicker access to capital for small businesses impacted by the COVID-19 pandemic.

"With the introduction of the Paycheck Protection Program, SBA shops essentially experienced 200 times the typical volume of loan requests versus what they are used to.

David Brooks, founder and CEO, Cirrus"

"With the introduction of the Paycheck Protection Program, SBA shops essentially experienced 200 times the typical volume of loan requests versus what they are used to," Cirrus founder and CEO **David Brooks** said.

"Cirrus' portal plays a key role in expediting the process of managing SBA loans, enabling Berkshire Bank to collaborate remotely, execute rapidly and scale quickly to efficiently address the influx in loan requests and alleviate the document chaos associated with SBA lending."

Berkshire also recently announced it has been working with Narmi to deliver a frictionless digital account opening experience to better serve customers with a quicker process that leverages the highest security standards.

Narmi said its platform is a deep integration with Alloy, an operating system for identity which manages all related fraud, compliance, and risk decisioning.

Berkshire said it now can securely and automatically decision all digital account openings. It said qualified applicants are approved quickly with the comfort of using an intuitive state-of-the-art fraud detection system. Together with Narmi, Berkshire offers non-document-based verification, integrated with data sources to verify applicants, administrator visibility and control to ensure the bank is satisfying compliance guidelines.

"Narmi has been instrumental in helping us move toward our goal of being a leader in 21st-century community banking," Berkshire Bank acting President and CEO **Sean Gray** said. "Narmi's digital-first and innovative account opening experience will drive organic growth in new accounts while delivering a best-in-class customer and staff user experience."

The bank said since it has been using Narmi's platform, it has an average time to complete applications of two minutes and 13 seconds, four times faster than the industry average; a 57 percent decrease in application time; and a 100 percent account funding rate.

"We're proud to align with Berkshire Bank to develop and launch an enterprise-grade account opening solution that will accelerate customer and deposit growth in an organic and responsible fashion," Narmi co-founder **Nikhil Lakhanpal** said. "Most importantly, our extensive experience with core banking systems and user-centric design allows Berkshire to offer an exceptional, seamless account opening experience to its customers."

Pacific Western Bank recently chose Treasury Prime as its technology provider to modernize its banking stack, the bank announced.

Working with Treasury Prime, Pacific Western Bank said it will be able to offer API access to its banking systems as well as a digital platform for clients like fintech

companies that want to embed banking services into their applications.

"Pacific Western Bank, through its various business lines including its Venture Banking group, provides banking solutions to leading innovative companies across the country," Pacific Western Bank Chief Operating Officer **Mark Yung** said. "As we embark on our own digital innovation journey, Treasury Prime impressed us with their technology as well as their deep knowledge of banking systems and processes. We're excited to partner with Treasury Prime to enhance our digital channels, and more importantly, to improve our client's experience."

Headquartered in Los Angeles, Pacific Western Bank has over $29 billion in assets. The bank provides community banking products, including lending and comprehensive deposit and treasury management services, national lending products including asset-based, equipment, real estate loans and treasury management services, and venture banking products.

"Treasury Prime works with the most innovative, forward-looking banks and we're proud to have been chosen by Pacific Western Bank to help them build their API strategy," Treasury Prime co-founder and CEO **Chris Dean** said. "Treasury Prime has a proven track record of working with banks to automate their backend processes and the API layer that we build to accelerate and automate internal processes can also be used by fintech clients or other companies that want embedded banking services."

Finicity recently launched a software that improves mortgage verification services, the company announced.

The new solution offers one-touch, GSE-accepted (government sponsored enterprises) and FCRA-compliant (free credit reporting act) verification of assets, income, and employment, reducing loan processing time by up to 12 days.

"We are streamlining mortgage lending significantly, reducing costs and shortening the time needed for the overall loan origination process," Finicity co-founder and CEO **Steve Smith** said. "With Finicity Lend, our ultimate goals are to help mitigate risk for lenders, create an improved consumer experience, and ultimately increase overall financial inclusion by helping borrowers better prove their creditworthiness."

The solution, called Mortgage Verification Service (MVS), allows consumers to permission data quickly and easily so lenders can verify assets, income, and employment in a single interaction, replacing a traditionally manual, paper-driven process. In addition to reducing the number of days required for processing, Finicity said MVS also would increase accuracy, improve profitability, and create a better experience for both lenders and borrowers.

National Mortgage Insurance Corp., the primary operating subsidiary of NMI Holdings, Inc., now is integrated with Mortech, a Zillow Group business. This integration brings National Mortgage's real-time, risk-based mortgage insurance pricing tool, Rate GPS to lenders.

"National MI is very pleased to integrate with Mortech, an industry leader in mortgage pricing technology," said **Norm Fitzgerald**, chief sales officer with National Mortgage. "Lenders and mortgage professionals leveraging Mortech's pricing engine will now have access to our competitive rates through our Rate GPS risk-based pricing tool, saving them time and streamlining the origination process."

Mortech said its product and pricing engine provides lenders with instant, accurate pricing at the click of a button, factoring in base price, servicing-released premium (SRP), loan-level price adjustments (LLPAs) and profit margin.

"We're excited to now offer lenders using our platform an enhanced and simplified process for obtaining competitive mortgage insurance premiums for their customers, all in one unified workflow," Mortech General Manager **Doug Foral** said. "This integration will help our lenders stay competitive in today's fast-paced mortgage environment."