



**FINANCIAL
SERVICES**

New boutique bank opens in Nashville with help from ImageQuest

Studio Bank is a boutique bank founded and located in Nashville, Tennessee. Studio Bank provides organizations, families, and individuals with sophisticated financial services through a multi-channel delivery model allowing clients to bank anywhere, anytime.

It's the first bank organized from the ground up in Nashville since 2008, according to American Banker and local media.

Founder Aaron Dorn, now the bank's Chairman, President & CEO, attracted capital from 400 investors, more than 85 percent of whom are in the Nashville area and contributed \$30 million of the \$46 million raised,



STUDIO
A BOUTIQUE BANK

THE COMPANY



Headquarters:
124 12th Ave. South,
Suite 400, Nashville, Tenn.



Founded: 2018



Initial Capitalization:
\$46 million



Website:
www.studiobank.com



Employees: 45

Founder: Aaron Dorn,
Chairman, President
& CEO (pictured)



"ImageQuest knew exactly what we needed," Dorris said. "Hardware was delivered on time and loaded with the necessary technology and software. They sat down with folks, set them up and got them working. They were very helpful in how we scaled our company."



according to The Tennessean. That reflects a strong local interest for a new local bank, Studio Bank officials say.

Many of Studio Bank's initial team worked at banks that had been bought by other, larger banks. They saw deposits in the market triple over an approximate 15 year period while the number of banks shrank during that same timeframe. That opened the door, Studio Bank organizers believe, for a new bank in Nashville.

"There were plenty of Nashvillians who missed the feel and personal touch of doing business with a truly local bank," said Chairman and CEO Aaron Dorn. "We are filling a pretty distinct need in the market. Even new Nashvillians want a bank that is local and authentic. We are providing that experience for our clients."

Although Dorn and other organizers began raising capital in 2017, the de novo bank faced regulatory hurdles it had to clear before gaining its state charter and approval from the Federal Deposit Insurance

Corporation. Bank officials said the start-up bank had to create more than 75 compliance, risk, and governance policies. Bank officials also had to develop the bank's business plans, financial forecasts, and information technology strategies.

IT COMPLIANCE

Helping Studio Bank with the regulatory review of its IT Compliance policies was ImageQuest's Milton Bartley. Bartley serves as Studio Bank's virtual Chief Information Security Officer, or vCISO.

A vCISO is an equivalent to a C-level executive who provides cybersecurity expertise as needed, similar to a fractional share of an asset. The vCISO can provide guidance to a company's board of directors.

Bartley assisted Studio Bank in meeting the FFIEC's regulatory requirements for risk assessment, policy development & compilation, business continuity measures, and the bank's overall cybersecurity maturity.



"Milton was at our side assisting with policy and procedure writing and navigating us through discussions with regulators," said Larry Dorris, Studio Bank's Chief Operating Officer. "He added tremendous value to the entire regulatory process."

Bartley also led the bank's first IT and security risk assessments, giving the bank a baseline from which to measure as it grows. Dorris said that help from ImageQuest was invaluable to the bank in its organization phase.

"Even though we're a young company, we still have big company cyber risks, so we need sophisticated risk mitigation," Dorris said. "Having this outsourced virtual CISO allows us to protect ourselves now and will continue as the company grows."

MANAGED IT

ImageQuest provided Studio Bank with an IT infrastructure designed to grow as the bank passed from its organizational startup phase to its Certificate of Authority to operate. Dorris said once the bank gained its regulatory approvals to open, hiring commenced and the bank's headcount grew significantly.

ImageQuest was able to keep up, providing desktops, software applications, and connectivity for the new mortgage bankers, commercial lenders, and bank operations employees.

"ImageQuest knew exactly what we needed," Dorris said. "Hardware was delivered on time and loaded with the necessary technology and software. They sat down with folks, set them up and got them working. They were very helpful in how we scaled our company."




*Larry Dorris, Studio Bank's
Chief Operating Officer*

"They do their job very well," Dorris said. "ImageQuest manages our local IT infrastructure, and they manage our Help Desk. When a Studio associate has an IT issue, they are talking to an ImageQuest associate."

Dorris said the ImageQuest Help Desk team works hard to help Studio Bank "with day to day troubleshooting and finding efficient ways to use technology. I give them high marks."

Dorris said his observations of and experience with ImageQuest further confirms that IQ is a competent company to scale with over time."

"They're transparent, they're affordable, and they have a lot of integrity. They're a good partner, a good advisor – and good at what they do." 



FFIEC regulates IT Security for Banks

Cybersecurity for Studio Bank is regulated by the FFIEC, or the Federal Financial Institutions Examination Council.


The council is a formal interagency body that works with the Federal Reserve Board of Governors, the Federal Deposit Insurance Corporation (FDIC), the Office of the Comptroller of the Currency (OCC), and the Consumer Financial Protection Bureau (CFPB).

The FFIEC works with all those agencies to create and enforce uniform principles, standards and reports from entities regulated by those agencies, such as banks and credit unions – including for cybersecurity.

There are specifically defined levels of risk in the FFIEC regulations and five specific areas that determine an institution's "maturity."

The FFIEC cyber regulations guide how banks and credit unions establish their "Inherent Risk Profile" and their "Cybersecurity Maturity." There are specifically defined levels of risk in the FFIEC regulations and five specific areas (or "domains") that determine an institution's "maturity." The domains include elements such as what the institution's network security controls are, what threats the institution may face, and how it would recover from a cyber incident, such as denial of service attack or a breach.

While that may sound relatively simple, the FFIEC Cybersecurity Assessment Tool requires many "declarative statements" from bank or credit union management that go into very specific details regarding an institution's cybersecurity posture.

What's more, the FFIEC expects "an institution's inherent risk profile and maturity levels will change over time as threats, vulnerabilities, and operational environments change." So banks and credit unions face regular reviews of their cybersecurity details. 



FFIEC

