NJ Banking Brief: All The Notable Legal Updates In Q1

By **Rosh Jaffe, Lisa Colone and Michelle Schaap** (April 1, 2024)

In this Expert Analysis series, attorneys provide quarterly recaps discussing the biggest developments in New Jersey banking regulation and policymaking.

New Jersey's banking and financial sector saw notable regulatory and legislative changes in the first quarter of 2024 as legislators advanced key reforms in cannabis banking, virtual currency and banking privacy.

This update will provide a look at some key developments of note from early 2024.


Rosh Jaffe


Lisa Colone


Michelle Schaap

Legislation to Protect Financial Institutions and Insurers Serving the Cannabis Industry

Despite the recent legalization of recreational cannabis in New Jersey, challenges remain for leaf-touching businesses and ancillary services in the cannabis industry seeking access to traditional banking and financial services as cannabis remains classified as an illegal drug on the federal level.

Accordingly, federally and state-regulated banks, credit unions, etc., remain without a clear regulatory and statutory framework on how to provide financial services to the legitimized cannabis industry in New Jersey without fear of scrutiny — from both state and federal regulators and from law enforcement.

In response to these challenges, on Jan. 9, Assemblywoman Verlina Reynolds-Jackson, D-Mercer, introduced A.B. 901, a proposed law aimed at protecting financial institutions and insurance companies engaged in business with the New Jersey cannabis industry.

If passed, A.B. 901 would provide a state-level safe haven for financial institutions authorized to engage in business in New Jersey. Specifically, Section 3 of A.B. 901 would, among other things, make the following changes:

- Ban any state agency or political subdivision from prohibiting, penalizing or discouraging any financial institution from serving any account holder purely because they engage in legitimate cannabis-related business; and
- Extinguish criminal liability for any financial institution — including its directors, officers, employees, agents, owners, shareholders or members — solely because it offers financial services to, or for the benefit of, a legitimate cannabis-related business or its business associates.

While A.B. 901, if passed, does not necessarily resolve the potential conflict with current applicable federal laws,[1] it would prove a major regulatory step forward in further legitimizing the provision of financial services to the cannabis industry in New Jersey.

NJ Bill Classifies Virtual Currencies As Securities Under Certain Circumstances

As uncertainty looms over whether digital currencies are properly considered to be securities under federal law,[2] New Jersey is one of at least 35 states that have recently introduced legislation concerning cryptocurrency, digital or virtual currencies, and other digital assets.[3]

Specifically, on Nov. 30, 2023, New Jersey Assemblyman Herb Conaway Jr., D-Burlington, introduced A.B. 5747, which "classifies all virtual currencies issued and sold to institutional investors as securities." The bill, which has been referred to the Assembly's Financial Institutions and Insurance Committee, would supplement the New Jersey Uniform Securities Law, which is silent on the topic of virtual currencies. The bill would also empower the New Jersey Bureau of Securities to adopt rules and regulations to effectuate the bill.

The bill states:

> "Virtual currency" means a digital asset that is:
>
> (1) used as a medium of exchange, unit of account, or store of value; and
>
> (2) not recognized as legal tender by the United States government.
>
> "Virtual currency" shall include a digital asset that is determined by the [New Jersey Bureau of Securities] to be a stablecoin.

The bill does not define the term "stablecoin," which Investopedia defines as "cryptocurrencies whose value is pegged, or tied, to that of another currency, commodity, or financial instrument."[4]

The bill defines an institutional investor as a "company or organization that invests money on behalf of other people, and includes, but is not limited to, banks, hedge funds, endowments, private equity firms, pension funds, and mutual funds."

There are two important practical implications of the bill.

1. The bill explicitly applies to institutional investors only.

In other words, the bill, curiously, does not cover retail investors.

As a result, even if the bill were to pass, the legal landscape in New Jersey would remain unclear as to whether virtual securities issued and sold to retail investors would be considered securities, and thereby subject to the authority of the New Jersey Bureau of Securities.

2. Were the bill to pass, it would be the law of New Jersey only.

The New Jersey bill would not resolve whether digital currencies are securities under federal law. And if the question is resolved on the federal level in the future, it could preempt New Jersey's determination in any event.

Privacy Considerations and Concerns for NJ Banks, Borrowers and Third-Party Service Providers

After several years and several failed, proposed bills, Gov. Phil Murphy signed into law the New Jersey Data Privacy Act, previously known as S.B. 332 and A.B. 1971, on Jan. 16. The NJDPA will become effective on Jan. 15, 2025.

The NJDPA applies to so-called controllers that conduct business in New Jersey, or produce products or services targeted to New Jersey residents, and that within a year

> a. control or process the personal data of at least 100,000 consumers, excluding personal data processed solely for the purpose of completing a payment transaction; or
>
> b. control or process the personal data of at least 25,000 consumers and the controller derives revenue, or receives a discount on the price of any goods or services, from the sale of personal data.[5]

While banks and other financial institutions are likely exempt from the NJDPA,[6] provided that they are subject to and in compliance with Title V of the federal Gramm-Leach-Bliley Act and with the Federal Trade Commission's Safeguards Rule, their borrowers may be subject to the NJDPA, regardless of whether they are for-profit enterprises. As such, banks should consider the NJDPA when evaluating and auditing their borrowers, and assessing such borrowers' compliance with their representations, warranties and covenants.

Further, while banks are already obligated to vet their service providers under the FTC Safeguards Rule,[7] and are required to contractually bind them to safeguard bank customers' data, bank service providers may soon have direct obligations if they are controllers subject to the NJDPA.

Unlike several other states' recently adopted data privacy laws, the NJDPA does not exclude nonprofits from its definition of controllers. Another feature that distinguishes the NJDPA from other states' privacy laws is its lack of threshold for the amount of revenue generated from the sale of personal data.

However, like privacy laws in other states, excepting California, the NJDPA excludes employment-related personal data and personal data processed in the context of a commercial transaction.

Given the type of information that banks' service providers may be processing, which may be deemed sensitive data,[8] these service providers may be subject to heightened obligations.

Banks will need their service providers to cooperate and coordinate with them. If a service provider receives a verified consumer request to forget consumer data, but for purposes of the banks the data is still needed, the service provider will need to respond to the consumer request by explaining why the data cannot be deleted.

While the NJDPA does not include a private cause of action, if a consumer were to suffer a data breach, and the data controller were subject to the NJDPA and failed to comply with the same, the controller could be subject to claims under Section 5 of the Federal Trade Act for unfair or deceptive acts or practices.

The data controller could also be subject to claims for violating New Jersey's Consumer Fraud Act (New Jersey Statutes, Section 56:8). Violations of the Consumer Fraud Act may result in fines of $10,000 for the first violation and $20,000 for subsequent violations. Further, the act allows consumers to bring an action for damages suffered as a result of a controller's violation.

Banks should consider the impact the NJDPA may have on service providers and borrowers.

Failure to properly vet service providers, whether pursuant to the Gramm-Leach-Bliley Act or the NJDPA, could result in claims against banks if their service providers are breached.

This was the case for Webster Bank in Christiani v. Guardian Analytics Inc. in 2023, after a ransomware attack on its fraud-detection service provider resulted in a data breach. While service provider Guardian Analytics notified Webster Bank of its breach in January 2023, Webster Bank did not notify impacted customers until April 20, 2023. This January, the U.S. District Court for the District of New Jersey approved a $1.4 million settlement between the bank and the affected account holders.[9]

While still unfolding as of the writing of this article, Bank of America notified customers this February that its technology partner Infosys McCamish Systems was the victim of a LockBit ransomware attack, exposing more than 57,000 customers' data. Notably, though Infosys compromised in fall 2023, Bank of America waited until February to inform affected customers.[10]

Banks should take note and review how they vet service providers and borrowers at onboarding and throughout their relationships.

Rosh H. Jaffe is a member at Chiesa Shahinian & Giantomasi PC.

Lisa M. Colone is a member at the firm and chairs the securities enforcement group. She previously served as vice president in the Financial Industry Regulatory Authority's Department of Enforcement.

Michelle A. Schaap is a member at Chiesa Shahinian and chairs the firm's tech, privacy and data innovations group.

[1] However, there is pending federal legislation that has a similar aim of A.B. 901, known as the Secure and Fair Enforcement Regulation, or SAFER, Banking Act.

[2] See, e.g., https://www.investopedia.com/news/how-sec-regs-will-change-cryptocurrency-markets.

[3] See https://www.ncsl.org/financial-services/cryptocurrency-digital-or-virtual-currency-and-digital-assets-2024-legislation.

[4] See https://www.investopedia.com/terms/s/stablecoin.asp.

[5] "Personally identifiable information" means any information linked or reasonably linkable to an identified or identifiable person. It does not include de-identified data or data that is publicly available.

[6] In addition to this exemption, the NJDPA also excludes entities covered by the Health Insurance Portability and Accountability Act of 1996 and the Health Information Technology for Economic and Clinical Health Act of 2009, and state and government agencies.

[7] The Safeguard Rule requires financial institutions to oversee service providers by:

> (1) Taking reasonable steps to select and retain service providers that are capable of maintaining appropriate safeguards for the customer information at issue;
>
> (2) Requiring … service providers by contract to implement and maintain such safeguards; and
>
> (3) Periodically assessing your service providers based on the risk they present and the continued adequacy of their safeguards.

16 C.F.R. Part 314.4(f).

[8] Under the NJDPA, "sensitive data" includes financial information, including a consumer's account number, account log-in, financial account, or credit or debit card number in combination with any required security code, access code or password that would provide access to the consumer's account. Additionally, "sensitive data" includes racial or ethnic origin, religious beliefs, mental or physical health condition, sexual orientation, citizenship or immigration status, genetic or biometric information, information from a known child, or precise geolocation data.

[9] Christiani v. Guardian Analytics Inc., Actimize Inc. and Webster Bank N.A., Case No. 2:23-cv-2158. According to the complaint, Guardian's database, in which Webster's customers' data was maintained, was not password protected, nor was it secured by multifactor authentication, and the data in the database was not encrypted.

[10] Bank of America Informs Customers About 90-Day-Old Cyber Attack – Forbes Advisor; Bank of America warns customers of data breach after vendor hack (bleepingcomputer.com). https://www.forbes.com/advisor/personal-finance/data-breach-affects-bank-of-america-customers/.