BakerHostetler

Brief

Change and Challenge

What's Next for the Financial Services Industry

November 2019

On Oct. 25, 2019, BakerHostetler's Financial Services industry team, in collaboration with the Ohio Bankers League, held its third Financial Services Summit in Columbus, Ohio. The speakers included Ohio Senator Sherrod Brown and leading attorneys and financial services executives. The summit featured panels on developments in cybersecurity and financial technology, litigation, blockchain, and cannabis banking.

Here are some highlights from the summit.

State of the Ohio Banking Industry

Presenter:
***Michael Adelman**, President and CEO, Ohio Bankers League*

- The health of the Ohio banking industry is good and getting better, with 219 banks currently having a physical, deposit-taking presence in the state and 181 banks chartered and headquartered in Ohio.

- 2018 was a record year for Ohio banks, largely due to the federal tax cut, and 2019 remains strong as quarterly net income expanded, loan growth increased, assets have grown and the number of problem banks declined. Industry consolidation remains at a steady 3 percent annual rate.
- Current banking industry concerns include reform of the Community Reinvestment Act, a 1977 federal law under which banks are scored on how well they are meeting the credit needs of low- and moderate-income neighborhoods. A revised set of rules is under consideration by the Office of the Comptroller of Currency.
- Cannabis banking is a hot issue, and there remains a need for federal legislation to create a safe harbor for banking marijuana-related businesses (MRBs). (See further coverage of cannabis banking below.)
- Fraud, especially phishing, is a persistent problem.
- Banks need to rethink their business model as they become technology companies offering banking services. Financial technology companies are becoming partners to banks as the digitization of banking services continues. However, there is a significant cost of investment in technology, particularly for smaller institutions.
- Talent acquisition is a concern as a mostly older workforce begins to retire. Smaller communities are especially hard-hit by this trend. The lack of interest in banking careers may be due to a lack of knowledge about the range of job options and lingering reputational damage in the industry. To counter this, the Ohio Bankers League has begun a partnership with independent colleges to award scholarships and increase recruitment, including a program at Central State University.

Cybersecurity for Financial Institutions: What Does "Reasonable" Security Mean Now?

Presenters:
***Craig Hoffman**, Partner, BakerHostetler*
***Eulonda Skyles**, Partner, BakerHostetler*

- According to BakerHostetler's *2019 Data Security Incident Response Report*, the top five causes of data security incidents are phishing (37 percent), network intrusion (30 percent), inadvertent disclosure (12 percent), stolen/lost devices or records (10 percent) and system misconfiguration (3 percent).
- Banks must tackle data security technology at an enterprise level. It's no longer good enough to have just a chief information officer who understands data security.
- Pay attention to what's happening to other banks and other businesses, and be prepared. Be able to document your data security measures and processes so that in the event of a breach, you can demonstrate preparedness and "have a good story to tell."
- Ransomware has morphed, and now threat actors are collecting millions of dollars in ransom and causing significant business disruptions. However, ransomware thieves typically do deliver decryption keys once a ransom has been paid. There are now third-party companies that specialize in negotiating with ransomware thieves, facilitating the payment and collecting the key.
- Banks should run a ransom scenario and work through a plan ahead of time. Practice restoring backups and negotiating simultaneously. See which method works first and best.

- Many banks are decommissioning their server farms and moving to cloud storage, but the cloud is the source of many data breaches and system intrusions. In particular, data aggregators that pull data from multiple accounts for dashboards may inadvertently expose an institution.
- Assess your risk. While businesses want metrics that show risk, security company assessments may not be privileged information, so be careful about what you choose to assess. Involve your legal department.
- Other security best practices include tailoring your controls to the risk, categorizing the data by sensitivity, making changes in multifactor authentication protocols, benchmarking yourself against your peers and seeing whether you need to upgrade.
- Threat actors will evolve their malware to foil anti-virus programs. That's why there is no one solution to cyber intrusion; a multipronged approach is necessary.
- People are fallible and make mistakes. Security training for employees should be up to date and rigorous.
- Board engagement is necessary to make sure data security investments are tested, measured and appropriately allocated.

Litigation and Regulatory Update

Moderator:
***Lisa Ghannoum**, Partner, BakerHostetler*

Panelists:
***Tom Eck**, Deputy General Counsel, The Huntington National Bank*
***Aaron Stucky**, Assistant General Counsel and Vice President, Fifth Third Bank*
***Keesha Warmsby**, Associate and Co-Leader of the Regulatory, Compliance and Licensing Team, BakerHostetler*
***Paul Weick**, Assistant Vice President and Senior Counsel, Key Bank National Association and Key Investment Services LLC*

Topics covered include the following:

- Litigation trends, including consumer protection claims, both individual and class action claims under the Telephone Consumer Protection Act, and False Claims Act cases against financial institutions.
- The Consumer Financial Protection Bureau's (CFPB's) stance on mandatory consumer arbitration agreements.
- Regulation Best Interest and the upcoming compliance deadline of June 30, 2020.
- Preserving the attorney-client privilege in regulatory examinations, including the Bank Policy Institute's push to have regulators not ask for privileged information.
- *Seila Law LLC v. CFPB* and the constitutionality of the CFPB.
- The California Consumer Protection Act and its applicability to and impact on financial institutions that handle the personal information of California residents.

Home Equals Life: Expanding Affordable Housing, Expanding Opportunity

Presenter:
***Senator Sherrod Brown** (D-Ohio), ranking member, Senate Banking, Housing & Urban Affairs Committee*

*Introduced by **Steven Dettelbach**, Partner and Co-Leader of White Collar, Investigations and Securities Enforcement and Litigation Team, BakerHostetler*

Senator Brown focused his remarks on the importance of banking and the mortgage industry to the ability of lower- and moderate-income families to afford housing. He noted that housing is almost always the largest budget item for families, and while profitability is up, wages are flat and workers' share of income has fallen.

Senator Brown emphasized that the housing finance system must work for working families by providing access to better home financing options. "This is a solvable problem," he said. "It comes back to work. When work has dignity, everyone can afford a house." But, he emphasized, no single idea or organization can provide all the answers to housing problems.

He closed by noting, "Real estate is not just a commodity; it's an investment in our community."

Blockchain: Financial Services Applications and Legal Issues

Presenter:
***Robert Musiala**, Counsel, BakerHostetler*

- Blockchain is a decentralized distributed ledger. A standard ledger system requires that the central agent be trusted. If a bank verifies an electronic funds transfer, for example, that transfer is deemed to have been made even if one party or the other contends that it was not. A decentralized ledger is a database that is synchronized across a peer-to-peer network of computers. The ledger permanently records changes to the database using cryptographic hash-linked "blocks." When a transaction occurs, a block is added to the ledger, forming a sequential chain with previous transactions – thus the name blockchain. Each block contains a hash from the previous block, so each transaction can be validated by computers and viewed and affirmed by consensus among the participants in the network. No single party controls the data or the information. Every party can verify the records on the ledger directly, without relying on any central authority.
- Blockchain technology can offer greater efficiency, transparency and security than centralized, trust-based systems and processes. Every transaction on the blockchain is visible to anyone in the computer system. Each user on the blockchain has a unique alphanumeric address, and everyone on the network can monitor each transaction.
- Distributed ledger transactions also offer security advantages over those enabled by a central authority. Because the ledger is chronologically ordered and stored on many computers across the network, a "hack" of a distributed ledger would require simultaneous changes to data on all systems. The algorithms behind blockchains have (thus far) been very secure.

- There are several ongoing blockchain projects for financial institutions. R3, a consortium founded by more than 100 banks and tech firms, recently announced a partnership to develop a blockchain-powered cross-border payments solution. Bank of America has joined an R3 project that leverages the Corda blockchain for a new trade finance platform being built with sponsorship by more than 20 international banks.
- J.P. Morgan has created its own cryptocurrency, the JPM Coin, which represents U.S. dollars held in designated J.P. Morgan accounts.
- Settlement system Ripple has an approximately 10 percent stake in MoneyGram. The two firms announced a partnership that will seek to incorporate Ripple's xRapid product into MoneyGram's remittance systems. Ripple's xRapid platform leverages Ripple's XRP cryptocurrency. And earlier this year, PNC Financial Services joined Ripple's RippleNet payment network.
- Various U.S. agencies have defined cryptocurrencies as falling into a variety of asset classes, depending on the situation. Thus cryptocurrency may be treated as money, property, commodities or securities, depending on the agency.
- In March 2019, FinCEN published detailed guidance on the money service business status of certain crypto activities, defining "what is a money transmitter," although there are several categories that may or may not be money transmitters, depending on circumstances.
- It is important for banks to employ enhanced due diligence programs specifically tailored to the cryptocurrency industry if they want to take advantage of these new opportunities while mitigating risks.
- When a financial institution is considering banking a blockchain business, the bank's anti-money-laundering (AML) staff must have an appropriate level of understanding of the cryptocurrency market.

Overview of Legal Cannabis and Banking

Moderator:
***Albert Lin**, Counsel and Co-Leader of the Regulatory, Compliance and Licensing Team, BakerHostetler*

Panelists:
***Kevin Allard**, Superintendent, Ohio Department of Financial Institutions*
***Justin Hart**, Executive Vice President, Grow Ohio*
***Miriah Lee**, Regulatory Counsel, Ohio Credit Union League*

- Marijuana is illegal at the federal level; however, 30 states, including Ohio, and the District of Columbia have legalized medical marijuana. Ten states and the District of Columbia have legalized recreational marijuana. Public acceptance is accelerating and now exceeds 62 percent.
- The market for legal cannabis is projected to reach $16 billion in the United States by 2020. Current estimates of sales in states with legal medical marijuana range from $9.6 million to $633 million, but actual revenue has exceeded projections. After legalization, the U.S. market is expected to exceed $80 billion by 2030.
- The 2014-15 Cole Memos address federal marijuana crime policy and financial crime policy and say the federal government will not seek prosecution if MRBs comply with a list of eight federal priorities, which include prohibiting the funding of criminal enterprises and distribution to minors.
- When determining whether to charge financial institutions for banking marijuana-related activity, the 2014 Cole Memo says prosecutors should apply the eight enforcement priorities.

- FinCEN Guidance for banking MRBs relies on the Cole Memos and has been explicitly reaffirmed since the 2018 Sessions Memo. Financial institutions also have the obligation to perform enhanced due diligence, establish a regulatory structure specific to MRBs and fulfill some additional filing requirements. Financial institutions also must develop a Bank Secrecy Act (BSA) and AML compliance system that accounts for the MRB guidance from the Department of Justice (DOJ).
- The FinCEN Guidance also includes several priorities for customer due diligence, ranging from reviewing an MRB's state license application to developing an understanding of the normal activity for the business, including the types of products sold and the types of customers served.
- Marijuana-Limited suspicious activity reports (SARs) should be limited to identifying information about the subject and related parties, addresses, the fact that the SAR is being filed solely because the subject is engaged in an MRB, and the fact that no additional suspicious activity has been identified.
- Marijuana-Priority SARs should include information about the subject and related parties, addresses as well as details regarding the enforcement priorities the financial institution believes have been implicated, and the dates, amounts and other relevant details of the transactions involved in the suspicious activity.
- Marijuana-Termination SARs should be filed when the financial institution believes it can no longer maintain an effective BSA/AML compliance program by serving the MRB.
- The 2018 Sessions Memo rescinded all prior DOJ guidance specific to marijuana enforcement, but Treasury Guidance remains unchanged. Various legislative efforts have endorsed the FinCEN guidance and are seeking to codify protections for banks. Earlier this year, U.S. Attorney General William Barr said the DOJ position "would be not to upset settled expectations and the reliant interest that have arisen as a result of the Cole Memorandum."
- The Rohrabacher-Blumenauer Amendment limits the DOJ's spending related to enforcement activity targeting legal marijuana, and lack of monetary support limits the DOJ enforcement activity vis-à-vis medical marijuana.
- Under Ohio law, financial institutions have safe harbor from criminal prosecution as long as the bank serving the MRB is compliant with state law and has paid applicable Ohio taxes. There are currently three Ohio credit unions banking MRBs.
- Ohio has three primary types of licenses:
    - Grower.
    - Processor turning the leaf into oil that is infused into products, then shipped to a dispenser.
    - Dispenser selling the product under a pharmacy license to registered patients with paperwork from registered doctors.
- A financial institution considering banking an MRB may ask the Ohio departments of Commerce or Pharmacy for the status of the MRB's license, affiliated businesses or individuals; a copy of the license application; information relating to sales or volume of product; and compliance with past or pending violations of the Ohio Medical Marijuana Program.
- Risk assessment is vital. Before banking an MRB, a bank should evaluate its business objective, perform a risk assessment of the customer and understand its capacity to manage those risks effectively. Financial institutions have a duty to formulate and articulate their policies regarding MRBs.

- Banks should know whether an MRB is interacting with them. Educate the financial institution's board, and understand the complexities of the MRB industry. For example, serving a cultivator is different from serving a fertilizer company with an MRB as a client.
- Watch the money trail, and be sure you are banking clean funds. Ask the MRB for a detailed financial plan. Under Ohio law, financial institutions can see numbers "from seed to sale."
- Financial institutions should put a lot of thought into the compliance process. Ensure you have the resources to handle the research and monitoring required, without putting your customer base at risk.
- The tier approach helps define the level of MRB engagement. These are not state designations, but when a bank designates a business as an MRB, the SAR process kicks in.
  - Tier I MRBs: Direct MRBs that are involved in the production of legal cannabis. In Ohio, that includes cultivators, processors, dispensaries, laboratories and physicians.
  - Tier II MRBs: Focused on providing services to Tier I MRBs, and they derive substantial revenue from MRBs.
  - Tier III MRBs: MRBs are not a focus of the company, and their revenue from MRBs is not substantial.
  - Tier IV MRBs: MRBs are not a focus of the company, and there is de minimis revenue from MRBs.

Conclusion

"Change and Challenge: What's Next for the Financial Services Industry" presented a comprehensive look at many of the regulatory and legal issues affecting financial institutions in Ohio and provided a road map for future developments. For additional information on any of the subjects discussed above, please contact one of these BakerHostetler attorneys.

Financial Services Industry Key Contact

Brett A. Wall
T +1.216.861.7597
bwall@bakerlaw.com

Additional Contacts

Steven M. Dettelbach
T +1.216.861.7177
sdettelbach@bakerlaw.com

Karl Fanter
T +1.216.861.7918
kfanter@bakerlaw.com

Lisa M. Ghannoum
T +1.216.861.7872
lghannoum@bakerlaw.com

Craig A. Hoffman
T +1.513.929.3491
cahoffman@bakerlaw.com

Albert G. Lin
T +1.614.462.4732
alin@bakerlaw.com

Robert A. Musiala Jr.
T +1.312.416.8192
rmusiala@bakerlaw.com

Eulonda G. Skyles
T +1.202.861.1555
eskyles@bakerlaw.com

Keesha N. Warmsby
T +614.462.4772
kwarmsby@bakerlaw.com

13.11.19.17.26_p07