NELSON MULLINS

FINTECH UNIVERSITY: *FINTECH AND BANK REGULATIONS*

MARCH 5, 2024

WHY FINTECH IS HERE TO STAY:

Customer Acquisition Cost:

Retail Bank: $925 per account.

FinTech:

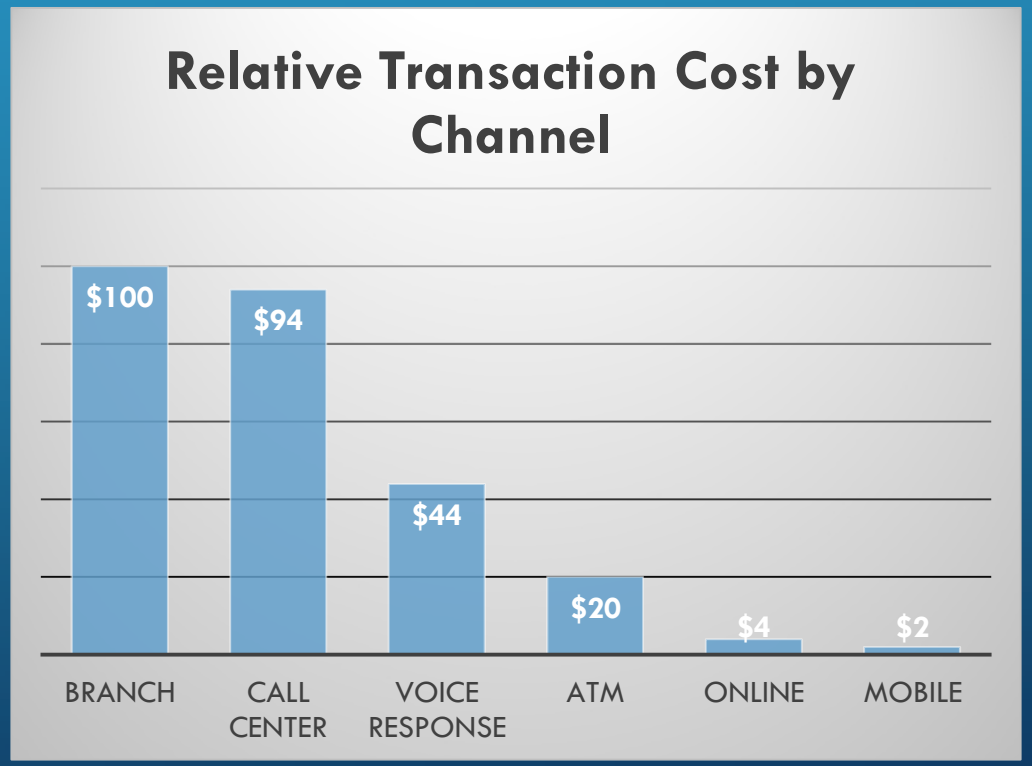
- Payments App: $10
- “Challenger Banks”: $30

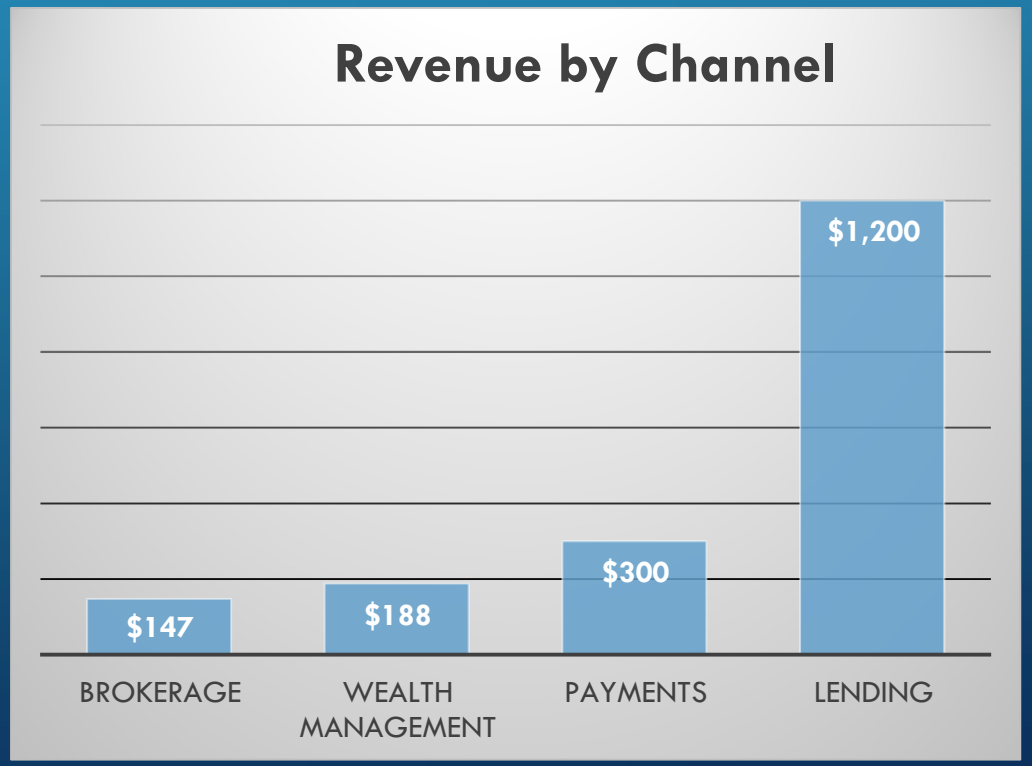
Lifetime Value:

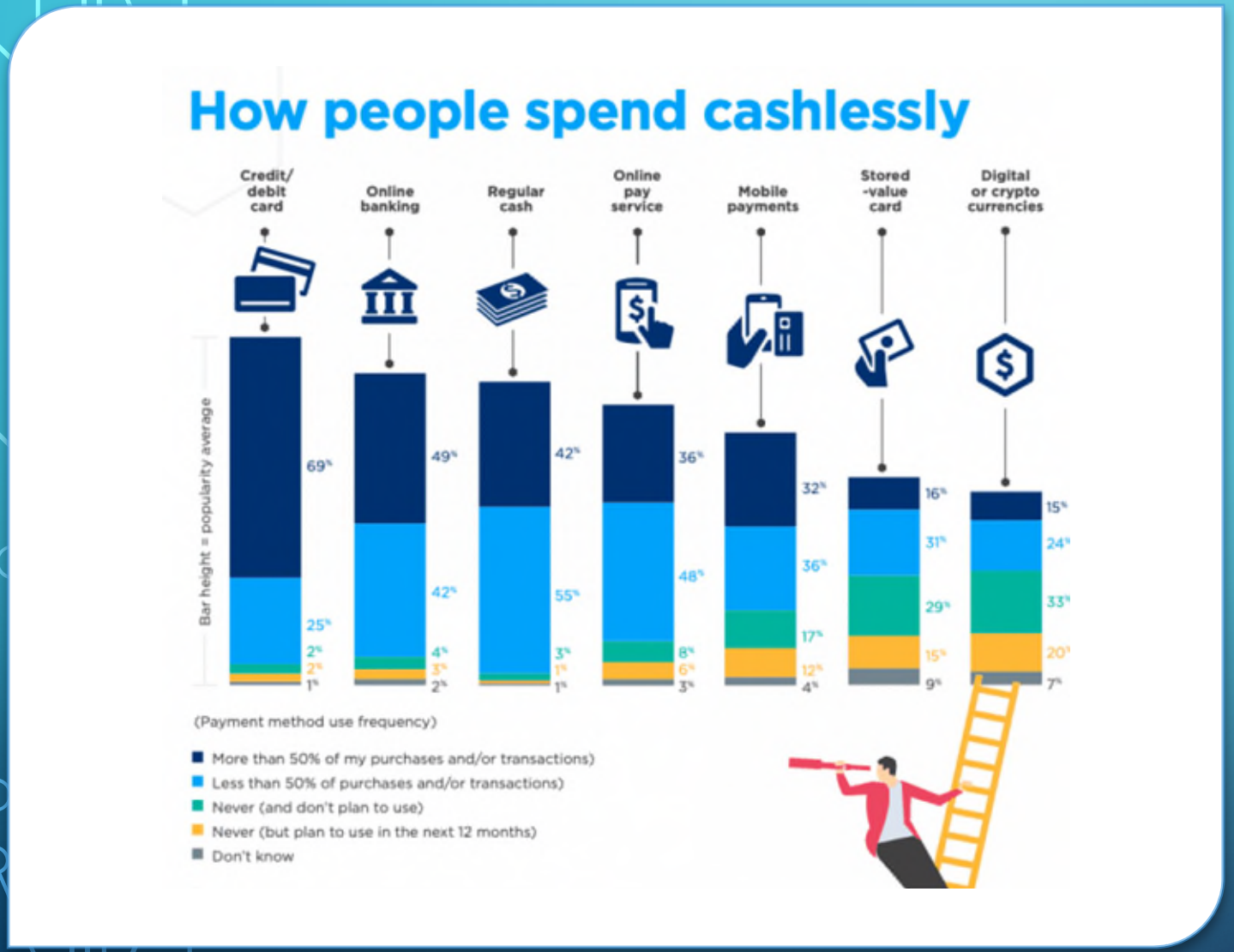
Payments App: $1,500

Retail Bank: $575

THE ECONOMICS OF TECHNOLOGY:







CONTINUED DRIVE TO TECH-ENABLED PAYMENTS:

**CrowdFund Insider (2020)

THE WARNING SIREN FOR BANKERS:

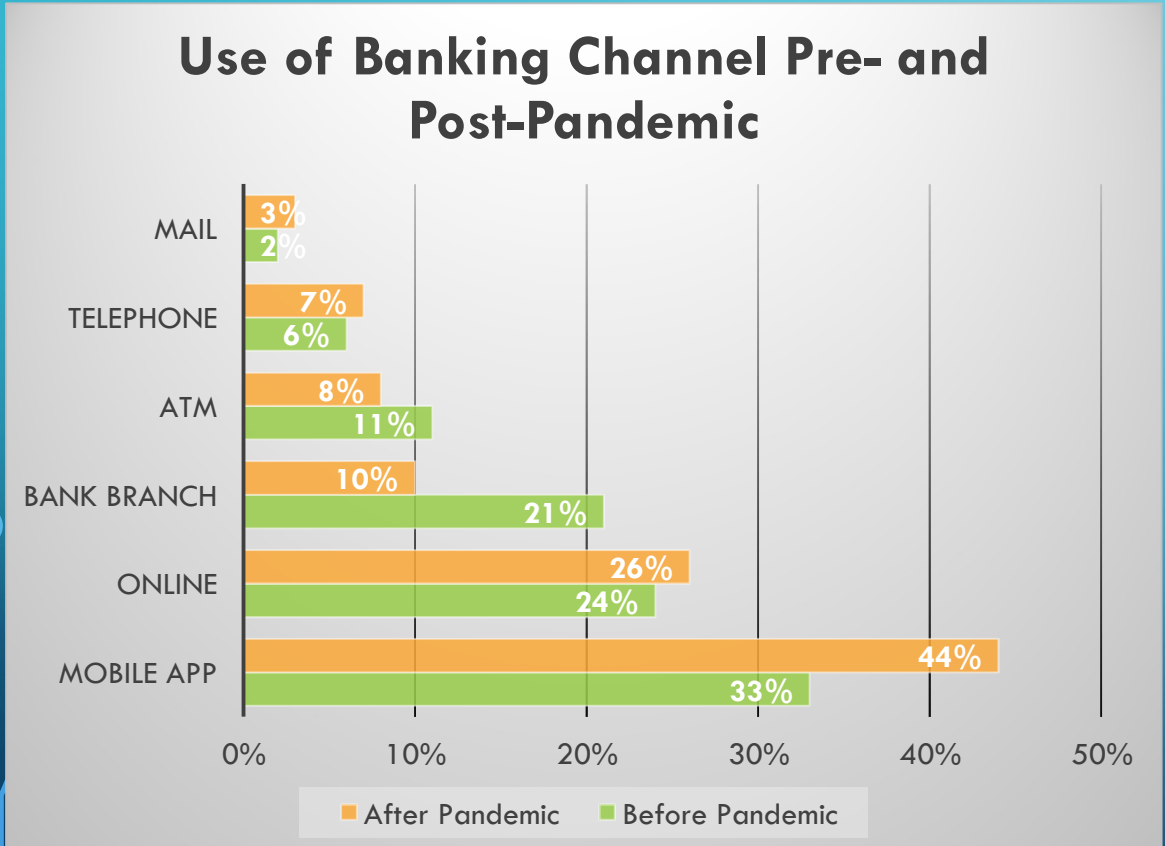
In 2019, **6%** of Consumers named a Fintech firm as their Primary Financial Institution.

By 2021, **31%** of Consumers named a Fintech firm as their Primary Financial Institution.

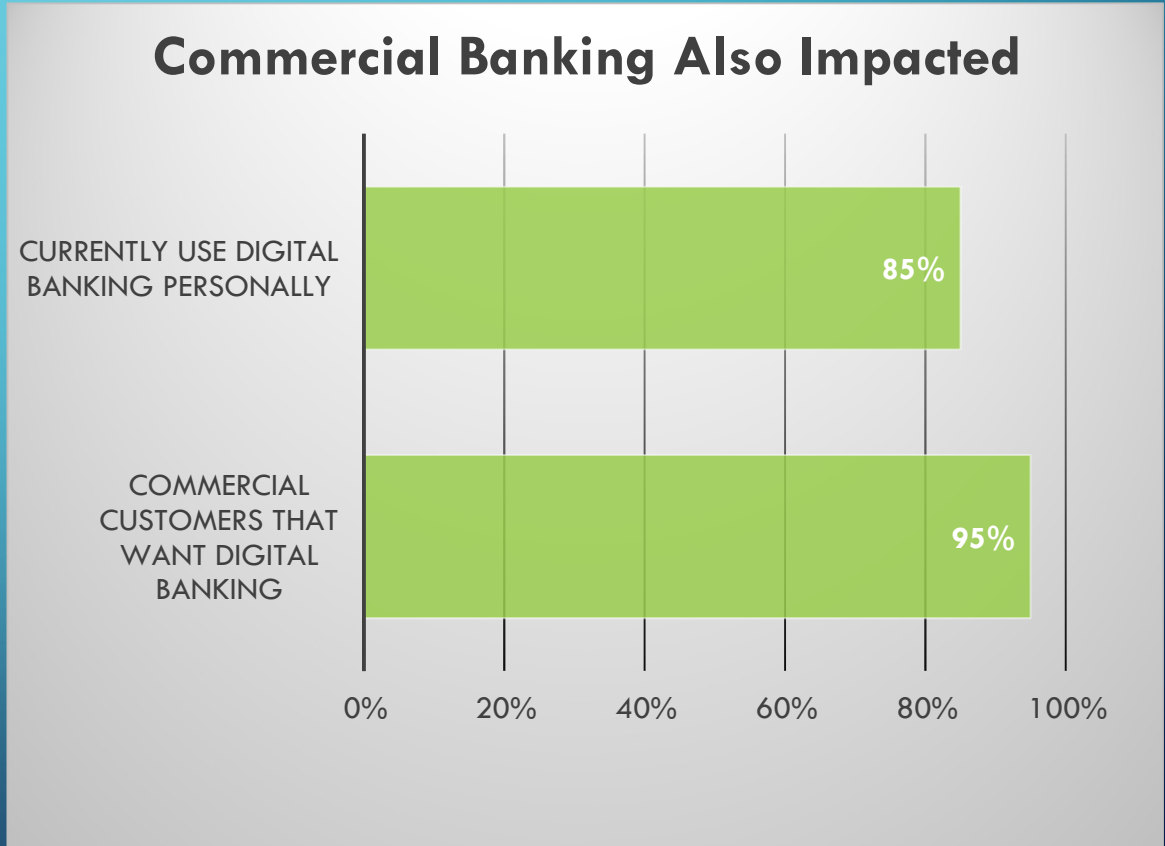
In fact, 51% of these consumers have set up direct deposit with a Fintech.

*Lele, Udiavar, and Mannamkery, *How financial institutions can win the battle for trust*, EY (2021).

DIGITAL TRANSFORMATION SPANS GENERATIONS AND CHANNELS



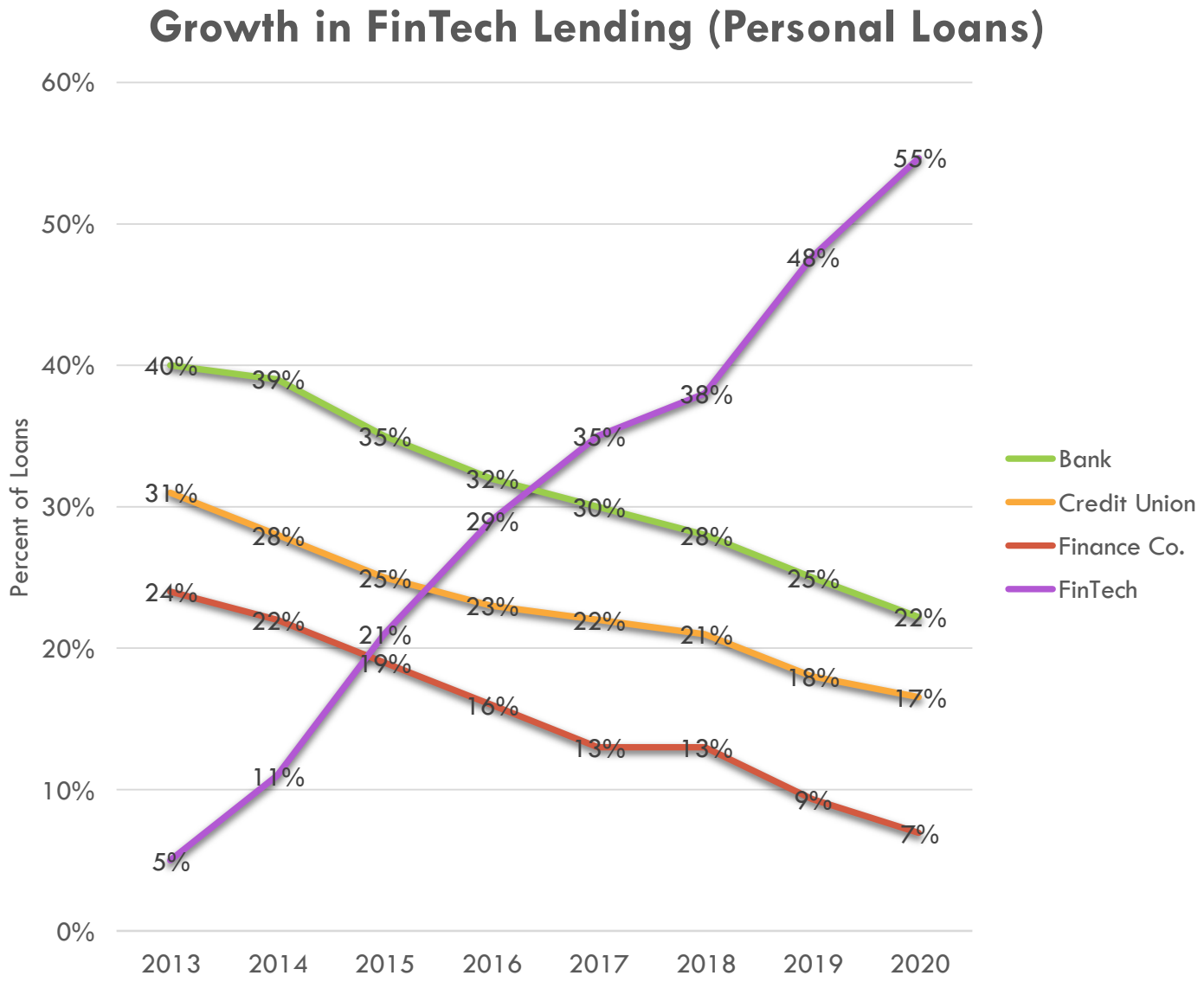
*Source: ABA (Feb. 2021)



*Source: Fraedom (2019)

THE DRAMATIC SHIFT IN LENDING

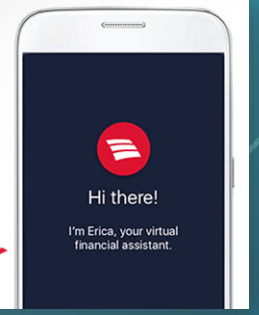
- *Source: TransUnion, *FinTechs Continue to Drive Personal Loan Growth*, Feb. 21, 2019 (2019 & 2020 projected using linear forecast).



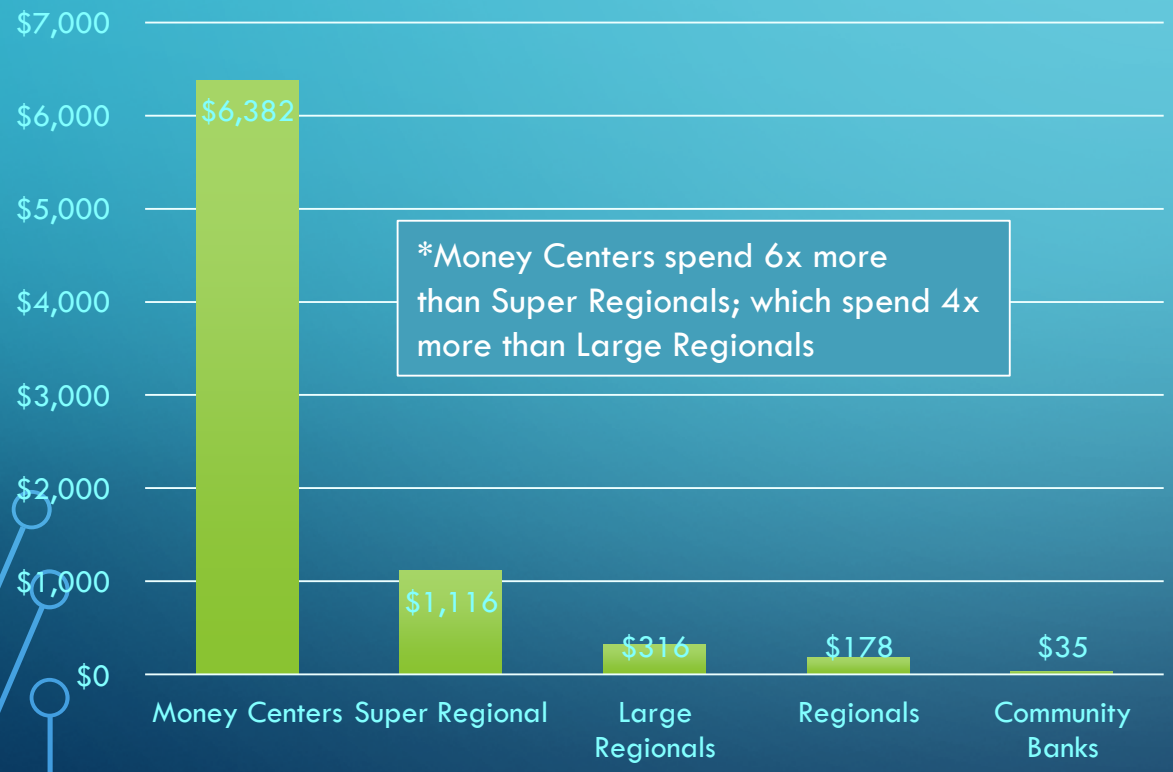
BANKING IN 2025

*BofA's Erica has resolved over 15MM customer inquiries in less than 6 months.

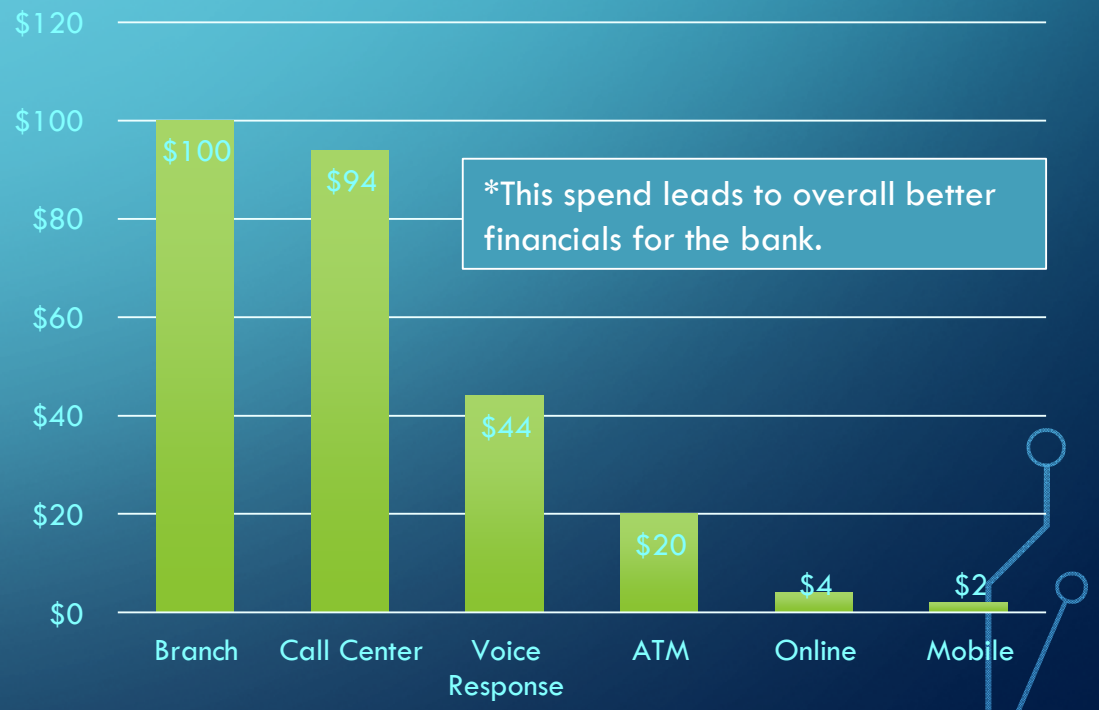
Bank of America



Average Technology Spend ($MM)

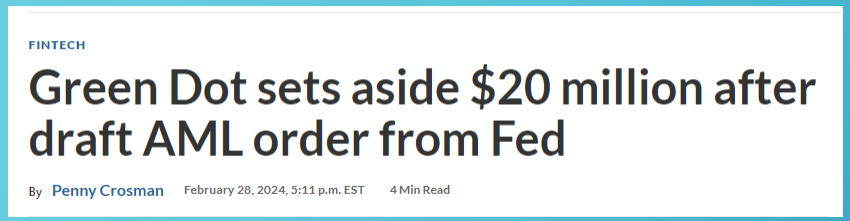


Relative Transaction Cost by Channel



FINTECH ≠ BAAS

- With recent scrutiny of bank-FinTech partnerships, many institutions do not differentiate the use of FinTech (or certain FinTech partnerships) from full banking-as-a-service.
- Bank-FinTech partnerships are a continuum. Different relationships can be appropriate for even the smallest banks.
- Structured properly, these collaborations *combine the strengths of both entities*—banks with their extensive balance sheets and regulatory knowledge, and fintechs with their innovative, flexible approaches and modern infrastructures.


FINTECH

Green Dot sets aside $20 million after draft AML order from Fed

By Penny Crosman February 28, 2024, 5:11 p.m. EST 4 Min Read

BANKINGDIVE

Tennessee bank hit with FDIC consent order over BaaS business

FDIC consent order with Cross River Bank indicates heightened scrutiny of bank-fintech partnerships

By **Ronald K. Vaske**, **John L. Culhane, Jr.** & **Richard J. Andreano, Jr.** on May 4, 2023

FINTECH

OCC says Blue Ridge in 'troubled condition' over BaaS

By Catherine Leffert January 26, 2024, 3:50 p.m. EST 3 Min Read

BANK TECHNOLOGY

'You're responsible. Period.' Banks take fire for fintech partnerships

By Catherine Leffert November 15, 2023, 4:11 p.m. EST 3 Min Read

BANK—FINTECH MODELS

Bank Referrals	• Bank earns revenue by sending customers to FinTech • Can be used where the bank has “gaps” in service offerings
FinTech Referrals	• Bank purchases customer leads from FinTech • Bank purchases account or loan assets originated inside FinTech platform
FinTech Investment or Acquisition	• Bank invests in FinTech that is mission aligned to bank • Bank buys key technology for private use or sale to other Financial Institutions.
Private Label Solution/SaaS	• Bank purchases the financial technology to deploy to its customers • Opens new product offerings for the bank
Bank to Bank	• Banks partner with each other to fill respective services gaps • Also includes relationships between technology and low-tech banks to offer services.
Partial Outsourcing	• FinTech assumes limited roles in process-underwriting, data collections, etc. • Allows the bank to “buy” technology or expertise missing in the institution
True “Bank Model Partnership”	• Bank serves as the lender/account issuer in FinTech themed ecosystem • Full integration in services with FinTech front-end and bank back-end

STRUCTURING PARTNERSHIPS

- Will the non-bank “white label” the product?
- Who will market?
- Who will underwrite?
- Who will decision and action applicants?
- Who will provide the originations platform?
- Who maintain account records?
- Who will service?
- Who will default service?
- Lending Relationship Structure:
  - Will the bank retain ownership of the loan? (Participation Model)
  - Will the bank transfer the loan? (Whole Loan Sale Model)
  - Will the bank obtain a funding line from the investor? (Warehouse Model)
  - Will the marketing entity be separate from the financial entity? (3-Party Model)
- Payment Relationship Structure:
  - Will the card be a prepaid card or white label debit card?
  - Will the bank maintain records or will a third-party ledger?
  - Who will serve as the program manager?
  - Who will handle Reg E disputes?
  - Will credit features be enabled?

DISSECTING THE CONSENT ORDERS

LESSONS LEARNED FROM CONSENT ORDERS AND REGULATORY GUIDANCE

COMMENTS OF ACTING COMPTROLLER MICHAEL HSU (FEBRUARY 21, 2024)

- The complexity of the relationships make regulatory oversight difficult.
- Banks must actively manage the risks of partnerships.
- FinTechs seeking banking charters will get no special treatment and will be treated the same as any other group seeking a charter.
- "Arguably, some FinTechs are already doing this, blurring the line between banks and nonbanks (and raising concerns about level playing fields)."
- Some FinTechs "started off simply facilitating payments," but now "offer customers the ability to deposit paychecks directly into their accounts, earn yield on the cash held there, and access credit, all with a few clicks of a mouse or taps on a phone."

THEMES IN RECENT CONSENT ORDERS

- Inadequate risk management
- Consumer protection failures
- Unclear monitoring responsibilities
- Inadequate board and management oversight
- Inadequate personnel and staffing
- Over-reliance on the FinTech's infrastructure
- Failure to monitor marketing and advertising
- Failure to review complaints and regulatory inquiries
- Failure to review FinTech's policies and procedures

CROSS RIVER BANK (MARCH 8, 2023 – FDIC)

- Maintain adequate records of who is providing banking services under CRB's charter
- Limits the addition to new programs without a non-objection from the FDIC
- Develop a program to assess each program's compliance with fair lending laws and regulations
- Develop technology that allows the bank to monitor each FinTech partner's program and analyze the partner's compliance with fair lending laws and lending regulations
- Conduct a risk assessment of each third-party relationship regarding fair lending and regulatory compliance
- Develop a robust fair lending internal control program and risk assessment to provide ongoing development of policies and procedures designed to:
  - address and mitigate any risks identified in the fair lending assessment,
  - require appropriate oversight and monitoring of all decisions made in connection with the marketing of credit programs, and
  - ensure fair lending compliance, and identify statistically significant disparities involving a prohibited basis.

FIRST FED BANK (NOVEMBER 21, 2023 – FDIC)

- Focused heavily on a relationship with Quin Venture – a "financial wellness" tool.
- The bank was accused of engaging in deceptive practices by implying that certain credit products were akin to unemployment insurance and misrepresenting fees and benefits associated with those products.
- First Fed is now required to submit a list of all credit and deposit products offered in collaboration with a third party
- First Fed must rebuild its policies and procedures, particularly for the:
  - Onboarding
  - Monitoring, and
  - Auditing of FinTech partnerships
- First Fed must review and approve copies of all third-party marketing materials
- First Fed must establish processes for managing regulatory agency inquiries, customer complaints and legal action
- First must review all third-party service providers' policies and practices to determine compliance with all consumer protection laws

CHOICE BANK (DECEMBER 18, 2023 – FDIC)

- Choice Bank must improve its board oversight of the bank's BSA/AML program and compliance, including for its FinTech programs (with, at a minimum, monthly oversight meetings)
- Redesign and establish an AML/CFT compliance committee and revise and strengthen the bank's AML/CFT program
- Rebuild and update the bank's internal controls
- Implement an appropriate customer identification program (CIP)
- Implement an appropriate customer due diligence program (CDD), including when these customers are onboarded through the partner FinTechs
- Implement appropriate suspicious activity monitoring and SAR reporting
- Engage in a lookback of past activity for possible corrective filings
- Ensure the bank has an appropriately sized staff with adequate resources and independence to meet the requirements of the order and the banking regulations

BLUE RIDGE BANK (JANUARY 29, 2024 - OCC)

- Maintain a committee to monitor the FinTech relationships and provide reporting to regulators
- Enhance the BSA/AML controls associated with the program
- Formalize a written program regarding risk management of third-party relationships
- Include formal plans to provide for SAR reporting
- Develop a strategic capital plan

LINEAGE BANK (JANUARY 30, 2024 – FDIC)

- Improve internal audit functions, focusing on high-risk areas such as deposits and payments obtained through third parties
- Establish a formal onboarding process that includes detailed due diligence and risk assessment for new FinTech partners
- No addition of new third-party relationships until a comprehensive third-party risk management program is in place
- Develop a contingency plan for terminating and winding up significant FinTech partnerships
- Must engage an independent firm to review its management structure and staff capabilities regarding BaaS oversight and risk management

GREENDOT BANK (MARCH 1, 2024 – PROPOSED CONSENT ORDER - FRB)

- Improve and formalize the bank's overall risk mitigation framework
- Establish a comprehensive compliance program
- Enhance its BSA/AML controls
- Conduct regular, independent reviews of its compliance monitoring programs
- GreenDot acknowledged that certain tech conversions had recently caused outages for a certain number of customers
- The Better Business Bureau had noted GreenDot had not responded to a "pattern of complaints" regarding locked accounts and lack of customer support.

THE INTERAGENCY GUIDANCE

THE BASE FRAMEWORK FOR FINTECH PARTNERSHIPS

INTERAGENCY GUIDANCE ON THIRD-PARTY RELATIONSHIPS: RISK MANAGEMENT (FDIC, FRB, OCC)

- **Risk-Based Approach**: The guidance endorses a risk-based approach for managing third-party relationships, which should align with the level of risk, complexity, and size of the banking organization, as well as the nature of the third-party relationship.
- **Lifecycle Management**: It covers all stages in the lifecycle of third-party relationships, including planning, due diligence, contract negotiation, ongoing monitoring, and termination.
- **Responsibility**: The use of third parties does not reduce a banking organization's obligation to perform all activities in a safe and sound manner, in compliance with applicable laws and regulations.
- **Risk Management Practices**: The document serves as a resource for banking organizations by providing examples of considerations and actions for each stage of managing third-party relationships.
- **Scope and Application**: While focusing on third-party relationships involving lending, payment, or deposit activities, the guidance clarifies that traditional bank-customer relationships are covered by existing risk management processes.
- **Regulatory Expectations**: It emphasizes the necessity for banking organizations to have robust risk management practices for third-party relationships, especially for those involving fintech companies.
- **Compliance and Controls**: Institutions are expected to review, develop, and implement appropriate policies and procedures for onboarding, monitoring, and auditing third-party fintech partners.

BREAKING IT DOWN

PLANNING

- Strategic Purpose
- Benefits and Risks
- Bank Staffing and Resources
- Volume and Financial Commitments
- Employee Resources and Management Experience
- Costs
- Board Oversight and Involvement

DUE DILIGENCE AND RISK IDENTIFICATION

- Subcontractors
- IT and Information Security Risks
- Consumer Impact
- Physical Security
- Bank's Capabilities
- Legal and Regulatory Compliance
- Risk Management Controls
- Operational Resilience
- Incident Reporting
- Complaint Management

THIRD-PARTY RELATIONSHIP SELECTION

- Strategies and Goals
- Financial Condition
- Business Experience
- Key Personnel and Experience
- Reliance on Subcontractors
- Insurance Requirements

CONTRACT NEGOTIATION

- Nature and Scope of Relationship
- Performance Measures
- Information Exchange
- Audit and Remediation Obligations
- Compliance with Laws and Regulations
- Costs and Compensation
- Ownership of Data
- Operational Resilience and Business Continuity
- Confidentiality
- Indemnification and Liability Limits
- Insurance Requirements
- Customer Complaints
- Use of Subcontractors and Use of Foreign Resources
- Default, Termination, and Wind-Down
- Regulatory Supervision

ONGOING MONITORING AND TESTING

- Review of Partner's Reports
- Effectiveness of Controls
- Ongoing Meetings and Performance Reviews
- Test of Controls for Higher-Risk Activities
- Change Management Controls
- Reviews of Financial Condition and
- Review of Insurance Coverage
- Testing of Compliance with Contractual Obligations
- Review of Compliance with Laws and Regulations
- Training Provided to Employees / Customer Support Functions
- Review of Ongoing Updates to Account for Changing Laws/Regulations/Threats
- Response to Incidents/Service Outages/Continuity Challenges
- Customer Complaints/Trends/Responses

TERMINATION AND WIND-UP

- Plan for Transition of Services
- Plan for Other Third Parties to Take Over Services
- Challenges and Timeline of Transition
- Costs and Fees Associated with Termination
- Costs and Fees for Data Retention and Data Translation
- Joint Intellectual Property and Data Transfers/Uses
- Risks to Other Operations/Customers of the Bank

STRUCTURING BANK GOVERNANCE

- Does the bank have oversight and accountability controls?
- Are relationships managed consistent with a FinTech charter or stated risk appetite?
- Are FinTech risk paradigms properly defined?
- Is the FinTech group siloed or part of an overall bank operational, compliance, and risk management system?
- Is there adequate reporting to inform management and the board of the risks and successes/failures of the partnerships?
- Do the bank and FinTech identify concerns, timely address them, and adequately remediate them?
- Does the bank have sufficient investment in the FinTech programs – external resources, internal experience, and compliance resources?
- Is the bank engaging in third-party, independent reviews of these relationships that inform the bank regarding its identified goals.

Fintech Nexus Newsletter (October 27, 2023): Synapse not firing on all cylinders

Peter Renton · Fintech Nexus Newsletter · Oct. 27, 2023 · 4 min read

Banking-as-a-service fintech Synapse is having a rough year, to say the least.

Earlier this month the company laid off 40% of its workforce, or 86 employees. This was on top of the 18% that the company laid off in June.

There is the now very public dispute they have been having with Evolve Bank & Trust, highlighted by Fintech Business Weekly. And they appear to have lost their largest client, Mercury.

Today, Forbes is reporting that Synapse and its clients need to be removed from Evolve's platform by December 31. According to Forbes, Synapse still has six FBO accounts for 40 clients at Evolve that will all need to be transitioned away in the next two months.

SYNAPSE EVOLVE

A CASE STUDY OF A FAILED FINTECH PARTNERSHIP AND PUBLIC FALLOUT

SYNAPSE

- A banking-as-a-service platform that provides payment, card issuance, deposits, lending, credit and investment products, and compliance.
- Used to extend Banks' back-end operations.
- In 2022,
  - Launched 2 new platforms (Global Cash and Modular Banking)
  - Cash flow positive
  - Passed 200 employees
  - Reached 18 million end users
  - Partnered with American Bank and Lineage Bank
- Clients have been complaining about poor user experience since 2020.
  - Empower (cash back on debit card purchases) switched providers
  - Oxygen left due to fraudulent activity that cost them hundreds of thousands of dollars
- Known to have little to no compliance monitoring.
- Partners with Evolve Bank and Trust for core financial functions – holding customer deposits.

EVOLVE

- Technology-focused financial services organization and BaaS provider that offers open banking, retail and commercial banking, mortgage lending, and SBA lending and trust.
- Self-styled global leader in payment processing.
- As of the end of 2022, held $1.3 billion in assets and $1.1 billion in deposits
- FDIC-insured bank based in West Memphis, TN
- Announced Partnership with Synapse in 2017.
- Accused of lending discrimination from 2014 – 2019
- Many high risk partners that have failed such as FTX, BlockFi, and Florifi.
- Sponsored numerous partners that have been investigated by different regulatory bodies.
    - Dave
    - Earnin'
    - SoLo (partners with Evolve through Synapse)

WHAT HAPPENED?

- In September 2023, Evolve Bank & Trust notified BaaS platform Synapse that it believed the company was in breach of contract. And on September 27th, Evolve informed Synapse of its intention to terminate the relationship.
- They have been having problems for a while. Reports of warning Evolve of a potential FBO account deficit since November 2022, but looks like this has been a problem since at least 2020.
- Currently, there is disagreement and an inability to reconcile over who was responsible for a discrepancy of $13M FBO accounts at Evolve holding customer funds.
- On September 27th, a letter sent by Synapse founder and **CEO Sankaet Pathak** to **Evolve Chairman and CEO, Scot Lenoir**, and **President of Open Banking, Hank Ward**, Pathak alleged an error on Evolve's part that led to a third-party payment processor incorrectly debiting an FBO account for at least $12M.
- There has been a combination of problems that led to the end of the partnership including voided checks that were settled when they should not have been; checks that had been marked settled but were then returned; checks that Synapse did not receive settlement for but should have; checks Synapse wanted to label as "do not honor"; and checks that were numbered "0."
- In just a week's span, Evolve failed to provide ACH Return files to Synapse, which resulted in approximately $3,492,910.61 being returned late. A loss of $82,416.33 loss for Synapse. Just a week sample, compared to the years of partnership.
- For months, Synapse and Evolve had been discussing moving to a new, tri-party structure, where fintech clients would contract directly with both Synapse and Evolve. The new structure would allow for better bank oversight of risks in the fintech programs. But in late September, Evolve and Mercury came to a deal, ultimately cutting out Synapse completely.
- Currently, Evolve has over $16M seized as collection of the deficiency and further protection for their End Users.
- The options presented as solutions were either Synapse reporting Evolve to the regulators and paying 1.5M instead of the 3.25M accidentally received from the FBO accounts or establishing a payment plan and winding down the partnership.
- As of October 6th, 2023, Synapse has issued major layoffs (40%) without severance payment.
- Evolve notified Synapse that it will cease its support of the platform by the end of 2023 and looks like it is currently in the process of dissolving the partnership.

ALLEGATIONS AND ISSUES: CHECK CLEARING

- Synapse and Evolve had no system to properly account for checks that had been voided or marked “settled” but subsequently returned.
- In addition, the technology had issues with checks marked “do not honor” or checks numbered as “0.”

check_number	transaction_id	transaction_status	transaction_status_note	transaction_status_date	transaction_amount	client_name	amount_match	return_post_date	description
[redacted]	62aa1c868c2d17e9023768ba	RETURNED	[Returned on Credit] Stop Payment	2022-07-05T20:23:09.743Z	11800	Mercury	FALSE	07/07/22	Check
	624d1efb4bc6393e604df3b8	RETURNED	[Returned on Credit] Payment Stopped	2022-07-05T22:15:40.991Z	10000	Relay	FALSE	07/13/22	Check
	626ac74b563dcf02df113cb8	RETURNED	[Returned on Credit] Stop Payment	2022-05-09T21:34:39.246Z	7985	Rho	FALSE	06/30/22	Check
	62e977579c94bf91e548726a	RETURNED	[Returned on Credit] CHRGI -- Stop payment	2022-08-12T14:19:34.736Z	6492.09	Mercury	FALSE	08/11/22	Check
	62756ee033cb09401b4d9574	RETURNED	[Returned on Credit] Stop Payment	2022-05-19T14:03:56.459Z	5000	Rho	FALSE	05/16/22	Check
	62b37121506834f82e73d	RETURNED	[Returned on Credit] Stop Payment	2022-07-12T19:09:25.388Z	5000	Mercury	FALSE	07/13/22	Check
	62daf00d8a0aecb3fc053f96	RETURNED	[Returned on Credit] Stop Payment	2022-07-25T21:16:14.203Z	5000	Mercury	FALSE	08/01/22	Check
	62dd7ef63bebfe181ac54e1d1	RETURNED	[Returned on Credit] Stop Payment	2022-07-25T21:16:24.253Z	5000	Mercury	FALSE	08/01/22	Check
	62977003ea67a0ceadce6ff	RETURNED	[Returned on Credit] Stop Payment	2022-06-27T16:39:26.982Z	4040.32	Mercury	FALSE	06/28/22	Check
	621d9bd18ba32b46defaf213	RETURNED	[Returned on Credit] Stop Payment	2022-05-30T04:07:05.804Z	3889.07	Mercury	FALSE	07/29/22	Check
	62f6ba9f6ba67f4627a6d1788	RETURNED	[Returned on Credit] Stop Payment	2022-05-31T21:09:39.827Z	2781.5	Mercury	FALSE	06/31/22	Check
	6287ca794e8b209a26227193	RETURNED	[Returned on Credit] Payment Stopped	2022-08-18T22:15:10.946Z	2244	Mercury	FALSE	08/19/22	Check
	620d0a45fb10c22af60defe	RETURNED	[Returned on Credit] Payment Stopped	2022-05-17T14:15:02.553Z	2159.75	Rho	FALSE	06/30/22	Check
	62cd0650b004c3d3ca4f50a8	RETURNED	[Returned on Credit] Stop Payment	2022-07-12T21:21:09.058Z	1080.33	Mercury	FALSE	07/29/22	Check
	62fa4d9f17e6d2f5b9427bf1	RETURNED	[Returned on Credit] Stop Payment	2022-05-21T19:15:21.475Z	1510.3	Mercury	FALSE	06/24/22	Check
	62d2d6d2935e14afba256d74d	RETURNED	[Returned on Credit] Stop Payment	2022-05-20T14:25:17.340Z	1360.32	Yolla Saving	FALSE	06/08/22	Check
	62a8d430caaa09c24c417ac	RETURNED	[Returned on Credit] Stop Payment	2022-06-21T15:05:52.608Z	1310.74	Rho	FALSE	06/24/22	Check
	62f3f2f9f7f4002fb70bccd9d9	RETURNED	[Returned on Credit] Stop Payment	2022-05-25T00:14:30.600Z	1000	CommonBond, I	FALSE	05/25/22	Check
	62d0602f949cc44b43d342c	RETURNED	[Returned on Credit] Stop Payment	2022-08-24T14:08:01.239Z	970	Alice	FALSE	08/25/22	Check
	6231f9521023b25a2f9cc73c	RETURNED	[Returned on Credit] Payment Stopped	2022-05-14T22:15:21.837Z	971.5	Relay	FALSE	06/16/22	Check
	62f6f963d7589d2feefcbbd7d0e	RETURNED	[Returned on Credit] Stop Payment	2022-05-09T21:56:24.176Z	775	Mercury	FALSE	05/03/22	Check
	62b1f18b862b4b18485e7fe72	RETURNED	[Returned on Credit] Stop Payment	2022-07-19T22:20:42.805Z	700	Snapl Spend,	FALSE	08/03/22	Check
	62b78b61042db47c9886ee4c	RETURNED	[Returned on Credit] Stop Payment	2022-07-06T00:35:25.206Z	625	Mercury	FALSE	07/07/22	Check
	618ed02fdfa3ccd3d95f67091	RETURNED	[Returned on Credit] Stop Payment	2022-05-04T14:02:04.974Z	621.06	Mercury	FALSE	05/04/22	Check
	629a707b124c71760fc8b877	RETURNED	[Returned on Credit] Stop Payment	2022-06-24T22:17:34.232Z	600	Mercury	FALSE	07/08/22	Check
	621e1356d0dc4412b23bf4b3	RETURNED	[Returned on Credit] Payment Stopped	2022-05-31T06:16:43.554Z	592.46	Rho	FALSE	06/24/22	Check
	6232eddbe321980ecfdcb5eb	RETURNED	[Returned on Credit] Stop Payment	2022-06-15T08:02:05.228Z	575.23	Mercury	FALSE	06/17/22	Check
	62dd880598ea7be600e537b	RETURNED	[Returned on Credit] Stop Payment	2022-07-06T19:49:47.480Z	500	Mercury	FALSE	07/13/22	Check
	62b1903bc44f72afaf93c303	RETURNED	[Returned on Credit] Stop Payment	2022-07-11T22:52:35.425Z	500	Mercury	FALSE	07/12/22	Check
	62c43c5ea9b9f99cbbd383	RETURNED	[Returned on Credit] Stop Payment	2022-07-11T22:53:18.399Z	500	Mercury	FALSE	07/12/22	Check
	620d5da149c8a214a26271dc	RETURNED	[Returned on Credit] Payment Stopped	2022-05-17T22:15:01.939Z	445	GROUNDWORK	FALSE	05/18/22	Check
	62d3662ec3cd98048aa03c8d	RETURNED	[Returned on Credit] Stop Payment	2022-08-24T14:08:08.254Z	348	Alice	FALSE	08/25/22	Check
	62c9e8514ad2955bafd2a191	RETURNED	[Returned on Credit] Stop Payment	2022-07-20T05:17:34.409Z	300	Relay	FALSE	08/05/22	Check

ALLEGATIONS AND ISSUES: ACH FILES

- Evolve's ACH department had failures that caused returned ACH files not to post to the Synapse system.
- Synapse worked with Evolve's outside accounting firm and found up to $6.5MM in ACH discrepancies in a single week period.
- Balance discrepancies between Evolve and Synapse "could differ a couple hundred million on the daily."

A. 248 ODFI ACH transactions totaling $6,180,767 missing from Evolve's feeds.
B. ACH Return ODFI missing 29 records amounting to $2,527.02.
C. Four RDFI ACH payments that appear to be two sets of duplicates in Evolve's feeds.
D. Seven RDFI ACH Returns, each displaying an amount $2.00 different from Synapse's records.
E. Four RDFI Check Deposits totaling $770.70 that were present in Evolve's feeds without authorization.
F. Twenty ODFI RDC transactions totaling $253,040.83, for which returns were provided to Synapse but are erroneously shown as settled transactions in Evolve's feeds.
G. Two ODFI RDC return transactions totaling $6,003.59, displaying amount mismatches.

ALLEGATIONS AND ISSUES: NO CONTROLS OVER THIRD-PARTY DEBITS

- Evolve allowed third parties to debit the master FBO account for fees and operating costs.
- Synapse alleges that a third-party payment processor, TabaPay incorrectly debited the FBO account for more than $12MM in a single day.
- Synapse claims this issues developed from a direct relationship that TabaPay started with Evolve in 2018 that predates the development of the Synapse program.

ALLEGATIONS AND ISSUES: DIRECT RELATIONSHIP WITH MERCURY

- By some accounts, the FinTech Mercury accounted for 70%+ of the Synapse deposit volume.
- Evolve had negotiated a separate, direct relationship with Mercury that would eliminate the need for Synapse.
- On September 25th, 2023, Synapse learned that Mercury would terminate its relationship with Synapse and move to a direct relationship with Evolve.

LESSONS LEARNED

- Internal reports show that both the bank and its FinTech partners were overly reliant on controls developed by Synapse – that may have failed or not had redundant oversight.
- In addition, Evolve is changing its strategy to refocus on "direct" FinTech relationships outside of integrators.
- Synapse used a unified FBO structure with multiple FinTechs, comingling funds into a single account. This created an overreliance on the Synapse infrastructure. (Synapse used 6 FBO accounts for 40+ clients).
- Accounts were used for both inbound and outbound funds, making tracing difficult.
- The FBO accounts also supported fee and revenue deductions, making tracing even more difficult.
- Synapse claims that Evolve immediately took a massive reserve that led to operational challenges at Synapse.
- Both companies immediately started making statements in public forums that led several FinTechs to spontaneously terminate relationships. (*Creating a Silicon Valley Bank-style run*).
- The parties were not regularly engaging in reconciliations of balances in accounts.

FALLOUT AND SUGGESTIONS

- Bank regulators are already questioning banks that overly rely on technology integrators to support their FinTech strategy.
- Regulators expect that banks *will not* rely on integrators for compliance and regulatory obligations.
- Banks will fully audit their FinTech relationships' account records and will constantly require reconciliation of accounts.
- All banks should have a business continuity plan that envisions the technology integrator's failure and inability to provide records of transactions or reconciliation of funds.
- Banks should refocus diligence on business continuity and disaster planning with the FinTechs, requiring formally documented procedures and ongoing monitoring/testing.
- As soon as problems are identified, the bank and the FinTech must immediately work to address the issues. (By some accounts, these issues were flagged as early as 2020).
- Banks should be clear on any exclusivity arrangements with the FinTech and consider how multiple banking partners may impact the bank's ability to reconcile and have visibility into accounts.

CHALLENGES IN THE REGULATION OF ARTIFICIAL INTELLIGENCE

HOW NEW TECHNOLOGIES ARE FAST OUTPACING REGULATORY GUIDANCE

WHAT IS ARTIFICIAL INTELLIGENCE?

Artificial Intelligence can be thought of broadly as any technology able to perform tasks that would typically require "human thought." This can be anything: (a) understanding something that is seen, (b) recognizing speech, (c) making data-driven decisions, (d) translating among languages, and (e) understanding risks of decisions.

Artificial Intelligence ("AI") encompasses two core concepts: (a) rule-based systems or (b) machine learning ("ML").

Financial services companies are already seeing AI enter the financial services sector. Each year, more FinTech firms are using AI to change how consumers view their relationship with financial services. Now, more than ever, customers expect easier, faster, 24-hour access to financial services.

CHATGPT: "HOW WILL AI CHANGE THE BANK OF 2030?"

1. Personalized customer service: AI-powered chatbots and virtual assistants could provide customers with personalized banking recommendations and advice based on their financial history and behavior.
2. Fraud detection: AI could be used to analyze large amounts of data and identify patterns and anomalies that could indicate fraudulent activity. This could help banks to prevent fraud before it happens.
3. Risk management: AI algorithms could be used to assess and manage risks associated with various financial products and services, including loans and investments.
4. Credit scoring: AI could be used to analyze a range of data sources and create more accurate credit scores for customers, which could help banks to make more informed lending decisions.
5. Compliance and regulation: AI could be used to automate regulatory compliance processes and ensure that banks are complying with relevant laws and regulations.
6. Investment management: AI algorithms could be used to analyze market data and make investment decisions on behalf of customers, based on their risk tolerance and investment goals.
7. Cybersecurity: AI could be used to detect and respond to cybersecurity threats, helping banks to protect their customers' data and financial assets.

Overall, AI has the potential to transform the banking industry in a number of ways by 2030, from enhancing customer experience to improving risk management and compliance. However, it will be important for banks to balance the potential benefits of AI with the need to maintain transparency, privacy, and ethical considerations.

THE EXPLOSIVE GROWTH OF AI:

Reporting, Compliance, & Operations:

- Auto clearing of false sanction screening hits generated by filtering software
- Auto booking of transactions and accounting entries on basis of unstructured data (voice log transcriptions, emails, forms…)
- Automatic reporting
- Increased sophistication of data analysis to better quantify risk
- Third-party vendor oversight and risk management
- Collections management

KYC & Data Protection:

- Big data analysis across systems to generate fraud alerts
- Suitability analysis for customers
- Automatic second line oversight of business units
- KYC reviews, including automatic screening
- Review of communications for possible data leaks
- Review of customer service interactions for prohibited conduct

Marketing & Sales:

- Targeted advertising for individual customers
- Customized product offers
- Real-time analysis of marketing effort ROI
- Real-time customer profitability analysis
- Customer prioritization
- Competitor usage analysis

Client Experience:

- Client satisfaction assessments
- Real-time client behavior patterns
- Real-time product recommendations
- Assessment of client “happiness” during bank interactions
- Early warnings for client dissatisfaction
- Early warnings for loan default
- Lower “marketing fatigue”

Predictive:

- Machine learning based underwriting
- Real time feedback on product design
- Missing solutions analysis
- Bigger data sets feeding customer risks assessments
- Cross-platform and inter-bank data ingestion
- Limit assessments

WHY?

Stronger Customer Relationships

End-to-end automation
24/7 Solutions
Highly-personalized banking experience

Higher Customer Lifetime Value

More effective cross-selling of financial products
Better understanding of ongoing customer needs

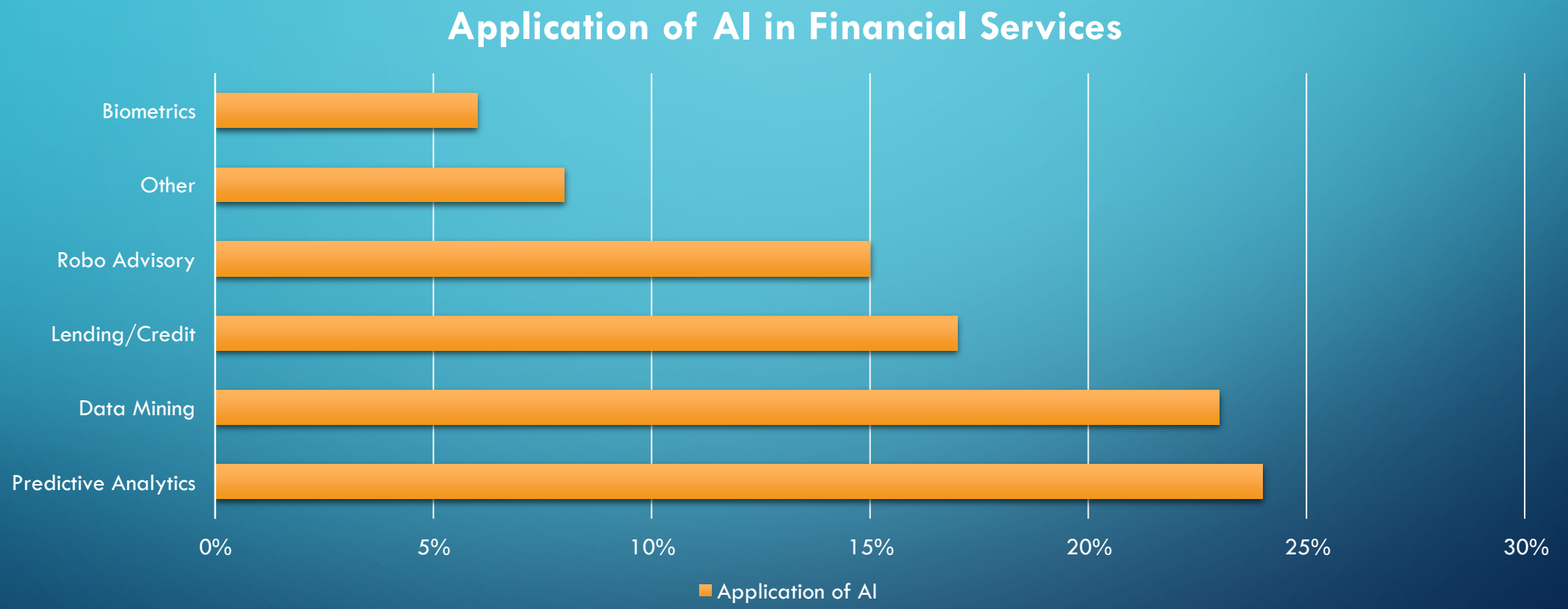
Lower Operating Costs

Shifting FTE workload to “higher” uses
Less document processing and review
More use of humans for the difficult, nuanced tasks

Lower Credit Risks

Bigger data sets
More predictive underwriting
Early detection of warning behaviors

HOW WILL WE USE AI?



*Goodwin, *A Global Survey of on the State of Financial Technology*

AN EMERGING REGULATORY FOCUS:

In a joint *Request for Information*, the prudential bank regulators (FDIC, Fed, OCC, NCUA, CFPB) sought industry feedback on the use of AI in banking. They identified several key use cases:

1. *Flagging unusual transactions*
2. *Personalization of customer services*
3. *Credit decisions*
4. *Risk management*
5. *Textual analysis*
6. *Cybersecurity*

The regulators also flagged a number of significant regulatory concerns — *more on that later….*

CUSTOMER STRATEGY

Servicing Strategy:

- Ranking of customers by “VAR”— value-at-risk (= Loan Value x Likelihood of Default)
- Routing to most appropriate servicers
- Using lower cost / lower resource tools for low-VAR customers (such as texts or automated calls)
- Using supervisors or best servicing staff for high-VAR customers

Customer Treatment Strategy:

- Often, the most difficult analysis is determining what strategy the bank should use for a given customer:
  - Customers with significant relationships with the bank (“custom” touch)
  - Customers who are “absent minded” (automated reminder systems)
  - Customers with high willingness, but low ability to pay (“restructuring” approach)
  - Customers with low willingness to pay and high ability to pay (“aggressive” collections)
  - Customers with low willingness to pay and low ability to pay (“early settlement and asset recovery” approach)
- Often, a computer can make these determinations much better than a bank collector.

CALL MONITORING

- Recent enforcement actions have revealed significant risks associated with third-party servicers, third-party debt collectors, and banking staff.
- Modern developments in language-based AI allows banks to monitor calls for “trigger words” for the compliance team.
- The newest technology can even track customer responses and effectiveness of tone and strategy.
- When this information is then cross-referenced to analytical data regarding accounts and products, it also allows you to monitor for over-pushing products or accounts.

"POINT OF DECISION" MARKETING

The *Harvard Business School (HBS)* spent significant time analyzing the "why" behind customer behavior. Traditionally, banks tried to understand their customers, their needs, and then match to these statements.

However, the HBS research revealed that most customers make decisions regarding a product based on a "problem" → "solution" approach.

HBS found that the single biggest driver of the use of a product was whether it was there when a client needed it and that it met their need at that point in time. This is extremely difficult for most businesses. However, through AI, this is now becoming realistic for banks.

Simply look at the buy-now-pay-later industry and you will see a great example of the explosive growth of *Point of Decision* financial products and their dramatic usage.

CHATBOTS AND NATURAL LANGUAGE AI

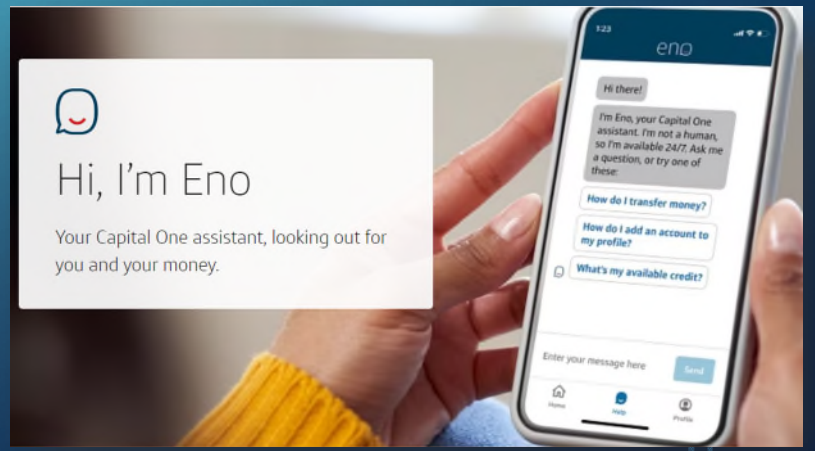
Already, text-based customer support is overtaking phone support.

Many times, the customer request is a simple status update or a simple transaction that takes a customer service representative <10 seconds. However, the customer is now on the phone for 5 to 10 minutes for a 3 second transaction.

Modern, natural-language chatbots are redefining customer service giving customers the “feel” of chatting with a human when the chatbot is truly responding.

Given customer usage, Chatbots are well positioned to serve customers (“Most Valuable Services”):

- Viewing statements and account balances (33% of respondents)
- Transferring funds between accounts (31%)
- Bill pay (28%)
- Peer-to-peer payments (11%)

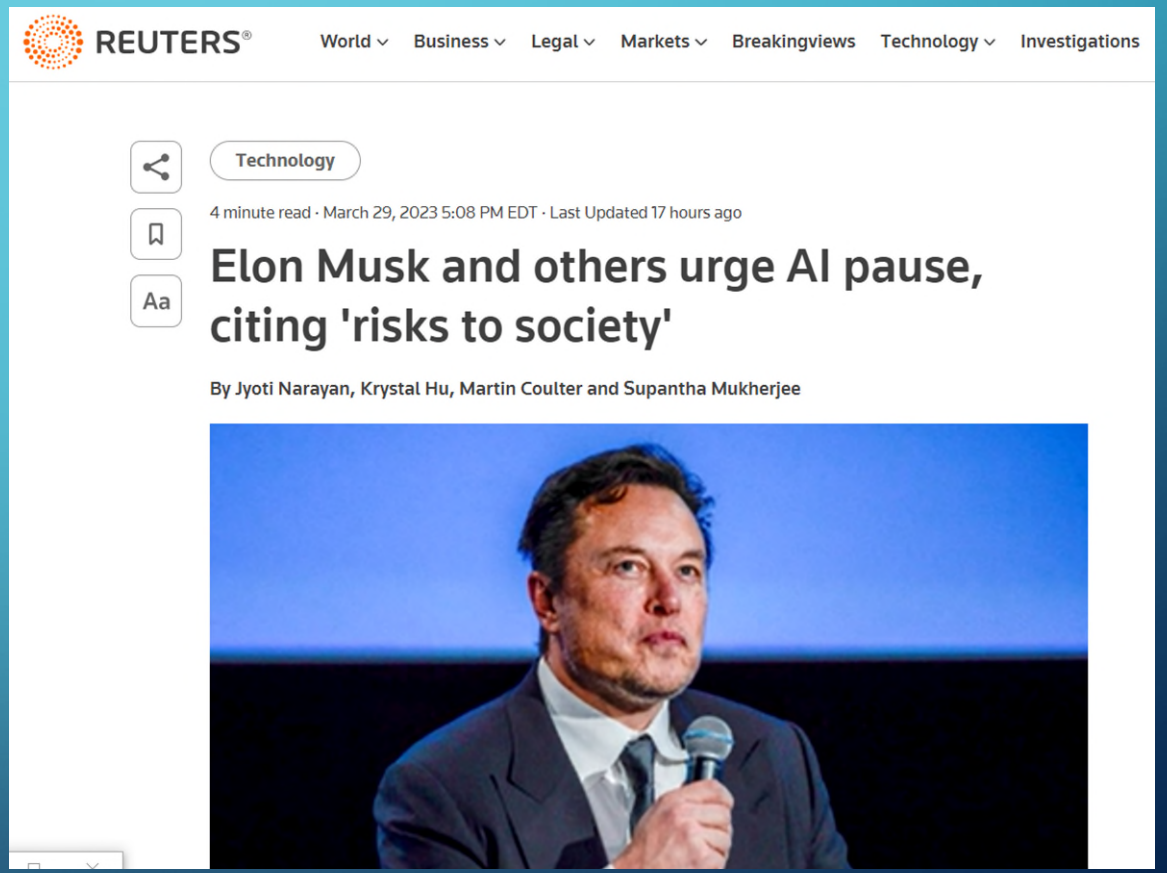


REGULATORY CHALLENGES

HOW FINANCIAL REGULATORS THINK ABOUT NEW CHALLENGES THAT ARISE WITH THE ENHANCED USE OF AI

SOCIETAL QUESTIONS…

- **Power**: GPT-4 can pass most AP exams and score in the 90th percentile of the Uniform Bar Exam taken by lawyers. One study found it can also promote misinformation and manage disinformation campaigns.
- **From the Letter:**
  - “Contemporary AI systems are now becoming human-competitive at general tasks, and we must ask ourselves: Should we let machines flood our information channels with propaganda and untruth?“
  - **"**Should we automate away all the jobs, including the fulfilling ones? Should we develop nonhuman minds that might eventually outnumber, outsmart, obsolete and replace us? Should we risk loss of control of our civilization?“
  - "Powerful AI systems should be developed only once we are confident that their effects will be positive, and their risks will be manageable."



ISSUES IN FINANCIAL SERVICES

Explainability: Without insight into an approach's general operating principles, bank management may not be able to evaluate with confidence how the system will function in unforeseen circumstances.

Data Integrity: Like other systems, AI is designed to interact directly with training data to identify correlations and patterns and use that information for prediction or categorization. If the training data are biased or incomplete, AI may incorporate those shortcomings into its predictions or categorizations.

Overfitting: "Overfitting" can occur when an algorithm "learns" from idiosyncratic patterns in the training data that are not representative of the population as a whole.

Cybersecurity Risks: AI may be exposed to risk from a variety of criminal cybersecurity threats. For example, AI can be vulnerable to "data poisoning attacks," which attempt to corrupt and contaminate training data to compromise the system's performance.

Dynamic Updating: Some AI has the ability to learn or evolve over time, especially as it captures new training data. This can cause drift as it learns from the new data. This can present challenges for validating, monitoring, tracking, and documenting the AI approach, including for persons conducting an independent review.

Third-Party Oversight: Given significant data exchange, TPRM programs are significantly more critical.

Fair Lending/Discrimination/UDAAP: Significant concerns have been raised with "black box" underwriting. There may be uncertainty about how less transparent and explainable AI approaches align with applicable consumer protection legal and regulatory frameworks, which often address fairness and transparency.

FTC GUIDANCE

- Be truthful about the claims the company can make through its use of AI software.
- Be truthful about the data the company uses.
- Be transparent about how AI software is used and what decisions are made using it.
- Take measures to establish oversight protocols for the use of AI software and its resulting outputs.
- Understand what data sets power the AI model to ensure it would not yield unfair or inequitable results to legally protected groups.

- Michael Atleson, *Keep your AI claims in check*, FTC (Feb. 27, 2023), https://www.ftc.gov/businessguidance/blog/2023/02/keep-your-ai-claims-check
- Elisa Jillson, *Aiming for truth, fairness, and equity in your company's use of AI*, FTC (Apr. 19, 2021), https://www.ftc.gov/businessguidance/blog/2021/04/aiming-truth-fairness-equity-your-companys-use-ai
- Andrew Smith, *Using Artificial Intelligence and Algorithms*, FTC (Apr. 9, 2020), https://www.ftc.gov/business-guidance/blog/2020/04/using-artificial-intelligence-and-algorithms

QUESTIONS THAT MUST BE CONSIDERED BY FINANCIAL SERVICES COMPANIES

- Is the source data legally obtained?
- Is the source data accurate?
- Are the sources the type that provides FCRA-level data or data actionable by a financial services company?
- Is the reporting agency complying with the FCRA and the FACT Act?
- Is the information being used in compliance with Fair Lending and UDAAP obligations?
- Is the data and its predictive results defensible/predictive?
- How will the company provide proper authorizations and obtain consent from consumers?
- How will the lender disclose adverse actions taken based on the data?
- How can a customer “fix” their standing with the company or improve the risk analysis?

THIRD-PARTY AI PROVIDERS

- When using third-party AI solutions, banks are expected to maintain oversight and accountability, ensuring third-party providers meet the same standards of safety and soundness.
- The use of third-party AI increases exposure to cyber risks. Banks need to enhance cybersecurity measures and protect sensitive customer data processed by AI systems.
- *How would your bank respond if your GLBA data was being provided in response to AI Chatbot queries?*

QUESTIONS OR FOLLOW UP?

Dowse B. ("Brad") Rustin IV

Chair, Financial Regulatory Practice

Brad.Rustin@nelsonmullins.com

202.689.2320 (DC)

864.373.2320 (SC)

www.nelsonmullins.com/people/dowse-rustin

QUESTIONS OR FOLLOW UP?

Craig Nazzaro

Partner, Financial Regulatory Practice

404.322.6969 (ATL)

Craig.Nazzaro@nelsonmullins.com

www.nelsonmullins.com/people/craig-nazzaro

QUESTIONS OR FOLLOW UP?

Kevin Tran

Partner, Financial Regulatory Practice

Kevin.Tran@nelsonmullins.com

615.664.5322 (NVL)

212.413.9000 (NY)

www.nelsonmullins.com/people/kevin-tran

QUESTIONS OR FOLLOW UP?

Elizabeth ("Liz") Donaldson

Partner, Financial Regulatory Practice

Liz.Donaldson@nelsonmullins.com

864.373.2248 (SC)

www.nelsonmullins.com/people/Elizabeth-donaldson

ABOUT THIS PRESENTATION

Nelson Mullins Riley & Scarborough LLP ("Nelson Mullins") provides this material for informational purposes only. Certain images, courtesy ChatGPT4.0.

The material provided herein is general and is not intended to be legal advice.

Nothing herein should be relied upon or used without consulting a lawyer to consider your specific circumstances, possible changes to applicable laws, rules and regulations, and other legal issues unique to your circumstances.

Receipt of this material does not establish an attorney-client relationship.

Nelson Mullins is very proud of the results we obtain for our clients, but you should know that past results do not guarantee future results; that every case or engagement is different and must be judged on its own merits; and that the choice of a lawyer is an important decision and should not be based solely upon advertisements or marketing materials.

Brad

Craig

Kevin

Liz

YOU STAYED TO THE END:

(*HOW AI VIEWS EACH OF US*)