

2022 WICPA FINANCIAL INSTITUTIONS CONFERENCE

YOUR SOURCE FOR KEY UPDATES & INSIGHTS ON TIMELY ISSUES

TUESDAY, MAY 10
BROOKFIELD CONFERENCE CENTER
& WICPA CPE LIVESTREAM



MATERIALS AT A GLANCE

The following materials are from the afternoon sessions of the 2022 WICPA Financial Institutions Conference held on Tuesday, May 10, including:

- Next Generation Banking: Technology Innovations Partnering With FinTech
- Prepare Now to Accelerate Your Business With Instant Payments & the FedNow Service
- Trends in Fraud & Financial Crime
- Ethics Update

**VIEW THOUSANDS OF ADDITIONAL IN-PERSON AND
ONLINE CPE OPPORTUNITIES AT [WICPA.ORG/CPECATALOG](https://www.wicpa.org/cpecatalog)**

Accelerate Business Growth with Simplified HR Management

Employ, enable and empower your workforce

isolated People Cloud is an intelligently connected human capital management platform designed to transform your organization by:



Providing a single solution to perform everyday HR tasks, eliminating the need for redundant data entries and improving organizational efficiency.



Minimizing risk with nimble software that is built to rapidly evolve with new industry requirements and regulations.



Delivering robust reporting functionality, including real-time labor data that can be used to make informed business decisions.



Offering consumer-grade technology that empowers employees to collaborate, which can improve productivity and engagement.

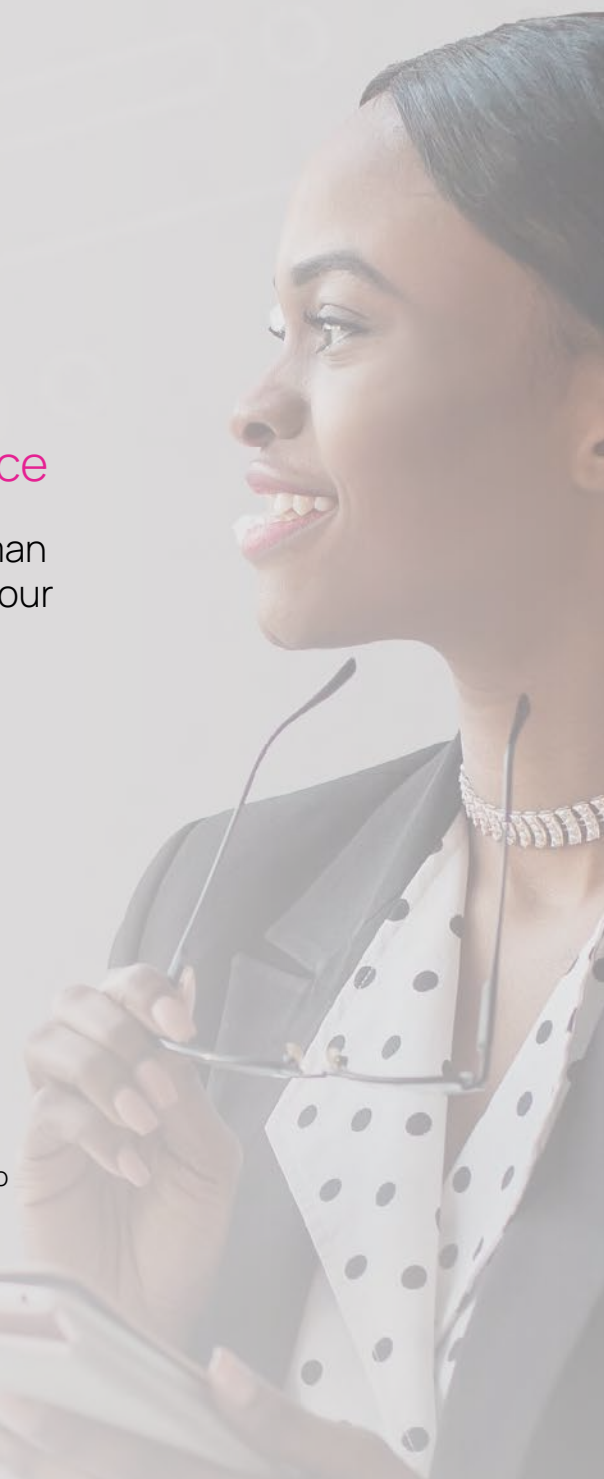


Streamlining and automating common HR tasks associated with payroll, scheduling, benefits enrollment and more.

Equip your team with isolated People Cloud and make it simple to manage the entire employee journey so more time can be spent focusing on strategic initiatives that impact your business's bottom line.

Learn more at isolatedhcm.com.

Or contact **Laura Martin** at lmartin@isolatedhcm.com or **314.495.3324**.





17th Annual

Retirement Plan Investment Seminar

Brookfield Conference Center

FREE EVENT

Wed. June 15th

8:15 AM – 12:15 PM

**Earn Continuing
Education Credit**

FIDUCIARY BEST PRACTICES | ECONOMIC UPDATE | MOTIVATION



Dave Sargent, CFA

Vice President, Fidelity Investments
Plan Sponsor Attitudes Survey



Emily Roland, CIMA

Co-Chief Investment Strategist, John Hancock Investment Management
Economic & Financial Markets Review



Steve Gilliland

Personal & Professional Development Expert, Steve Gilliland, Inc.
Detour: Developing the Mindset to Navigate Life's Turns

EARN CONTINUING EDUCATION CREDIT



4 CPE
Credits



4 PD
Credits



4 HR
Credits

Register Today



RSVP online at
<https://bit.ly/RP-Seminar-WICPA>

Spectrum Investment Advisors

(800) 242-4735 | www.spectruminvestor.com

WICPA, Fidelity Investments, John Hancock Investment Management and Steve Gilliland are not affiliated with Spectrum Investment Advisors.

For CPE credits, please call the CPE Department at 800-772-6939 or register thru the WICPA Website. / PD Credit program is valid for the SHRM-CPSM or SHRM-SCPSM / The use of the official HRCI seal confirms that this activity has met HR Certification Institute's® criteria for recertification credit pre-approval.

A photograph of a lighthouse on a rocky shore at sunset. The lighthouse is black and white striped with a glowing light at the top. A person is walking on a pier in the distance. The sky is a mix of orange, pink, and blue.

Bank on Wipfli

The Bank on Wipfli blog and podcast provides financial institutions with the latest news, insights, ideas and tips.

Tune in to meet **Robert Zondag**, our podcast host.

Subscribe for free.

wipfli.com/bankonwipfli-wicpa

WIPFLI

CONNECT



A GREAT WAY FOR WICPA MEMBERS TO COLLABORATE

WICPA Connect is your exclusive members-only networking and knowledge base designed to connect you with WICPA members and resources.

- **Network with peers** and grow your contact list using the member directory of more than 7,000 members.
- **Post questions** to find out from fellow members who have the expertise or may have been in the same situation.
- **Personalize your profile** by adding your interests, education, experience, honors and even your photo.
- **Contribute and download resources** such as documents, whitepapers, articles, reports, guides and more.
- **Share your knowledge and expertise** by answering questions and offering your insights and ideas to fellow members.
- **Customize your experience** with controls for profile visibility, discussion signatures, notifications and more.

As a WICPA member, you already have a profile on WICPA Connect.

Simply go to wicpa.org/connect and sign in using your existing website login information.

2022 WICPA GOLF OUTING

FRIDAY, SEPT. 16 – Ironwood Golf Course, Sussex



SCHEDULE

8:30 a.m.
Registration & Breakfast

9:00 a.m.
Practice Greens
& Driving Range

10:00 a.m.
Shotgun Start

144 PERSON LIMIT

4-Person Scramble
\$90 per Golfer
\$360 for Foursome

HOLE & EVENT PRIZES

\$500 Inside the Circle Contest
\$500+ in Individual Awards
\$500+ in Team Awards

REGISTRATION INCLUDES

18 Holes of Golf With Cart
Practice Greens & Driving Range
Continental Breakfast & Lunch
Beverage Vouchers
Hole & Event Prizes
Entry in the Raffle Drawings
Awards Reception & Appetizers

For more information and to register, visit wicpa.org/GolfOuting.



12:35 – 1:25 p.m.

Next Generation Banking: Technology Innovations Partnering With FinTech

**Marcie Bomberg-Montoya, OCI, OEI, Principal – Strategic Advisory
Services Leader, Wipfli LLP**



Next Generation Banking: Technology Innovations Partnering With FinTech

WICPA

Financial Institutions Conference

WIPFLI

“To keep up with the world of 2050, you will need to do more than merely invent new ideas and products, but above all, reinvent yourself again and again.”

Yuval Noah Harari



Agenda for Today

Banking Trends

FinTech, Banking as a Service, and Hyper Personalization

Forecasting the Future

Financial services after the pandemic

- World became digital overnight
 - Everything that could move online, did move online
- More work from home employees
 - Some will most likely not return to the traditional office
- Innovation is imperative
- Personal development will prepare employees for unforeseen circumstances
 - Keep up with technology
- Sustainability will be valued by Consumers and Stakeholders alike

FS Industry themes driving change

- Meeting the client where they want to be met (physical location or digital or both)
- Reexamination of the core business model – ability to profitably grow revenue
- Efficiency
- Focus and prioritization
- Hybrid work models
- Digital, digital, digital
- Consolidation is expected to accelerate

5

Trends to watch for 2022 and beyond

- Virtualization of the workforce – flexible workplace models
- Focus on safety and surveillance – higher consumer expectations driving increased spend on cybersecurity, data privacy, and data analytics
- Corporate responsibilities – the role of financial services companies is changing
- Emergence of pop-up ecosystems – creative partnerships
- Focus on cost reduction
- Digitization – further adoption of contactless technologies and digital experiences (ITMs, contactless kiosks, AI Robotics, virtual/augmented reality)
- Hyper personalization (more to come on this)

6

Strategic priorities for 2022 and beyond

- Growing/alternative revenue
- Efficiency/cost cutting
- Taxes and regulation
- Attracting and retaining talent
- WFH/Hybrid work/culture
- Current franchise value
- M & A, Board succession, and transition
- Corporate responsibility/DEI
- Brick and mortar v. digital
- Innovation (mindset)
- Client journey mapping
- Technology service providers
- Cyber, data privacy, data analytics
- Digital/tech planning
- Cryptocurrency
- Creative partnerships
- Relevance

7



FinTech

Banking as a Service

Hyper personalization

Evolving narrative of FinTech

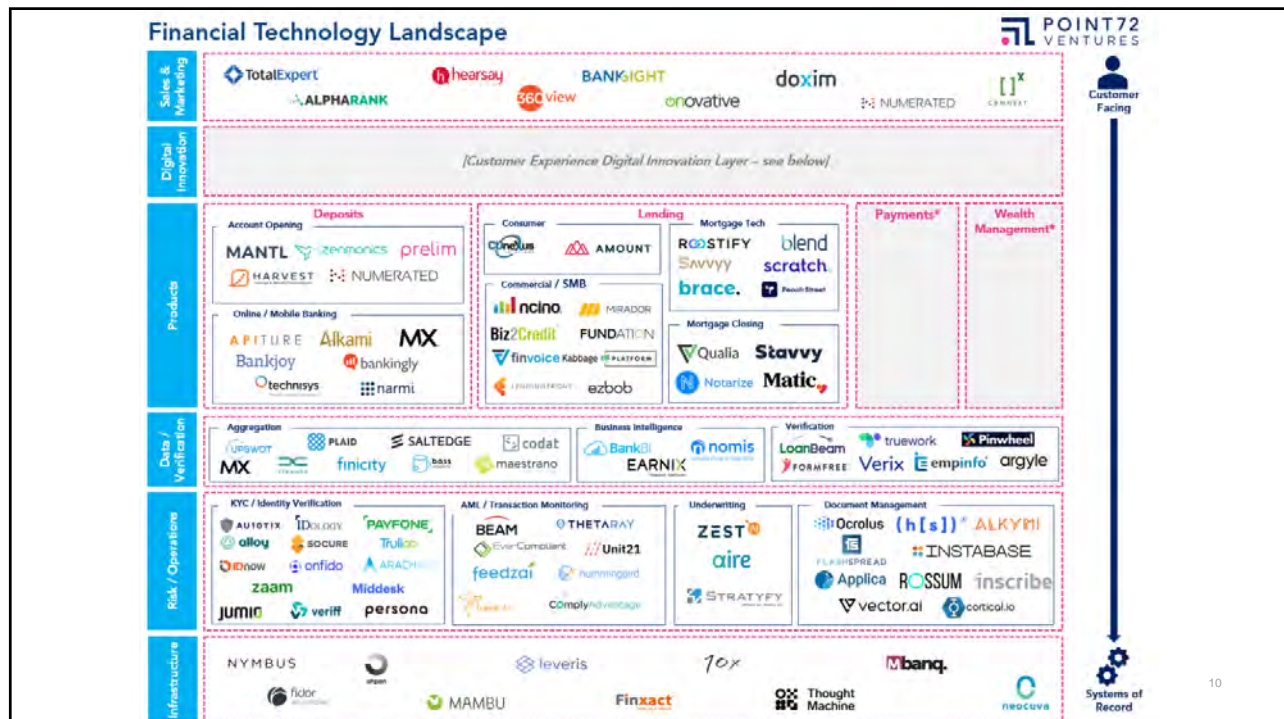
2016 - 2017 - 2018:

Competition, “not really” competition, initial collaboration, accelerator programs, investments and acquisition

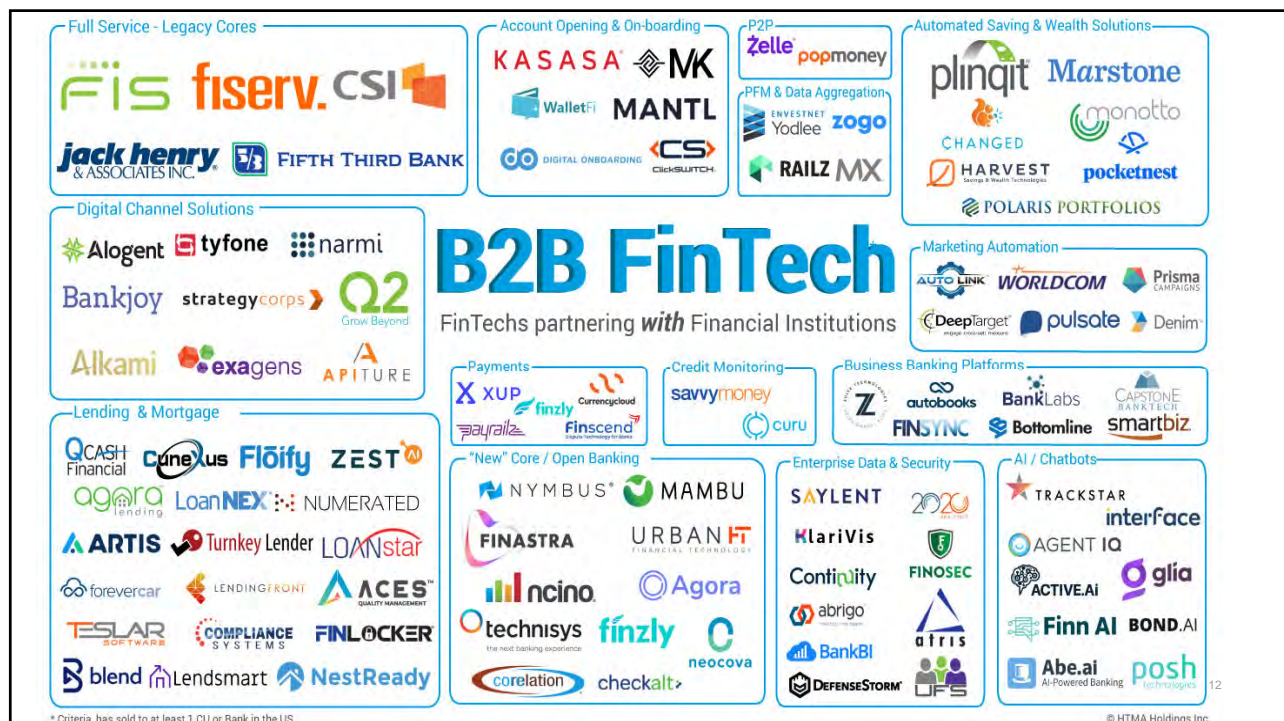
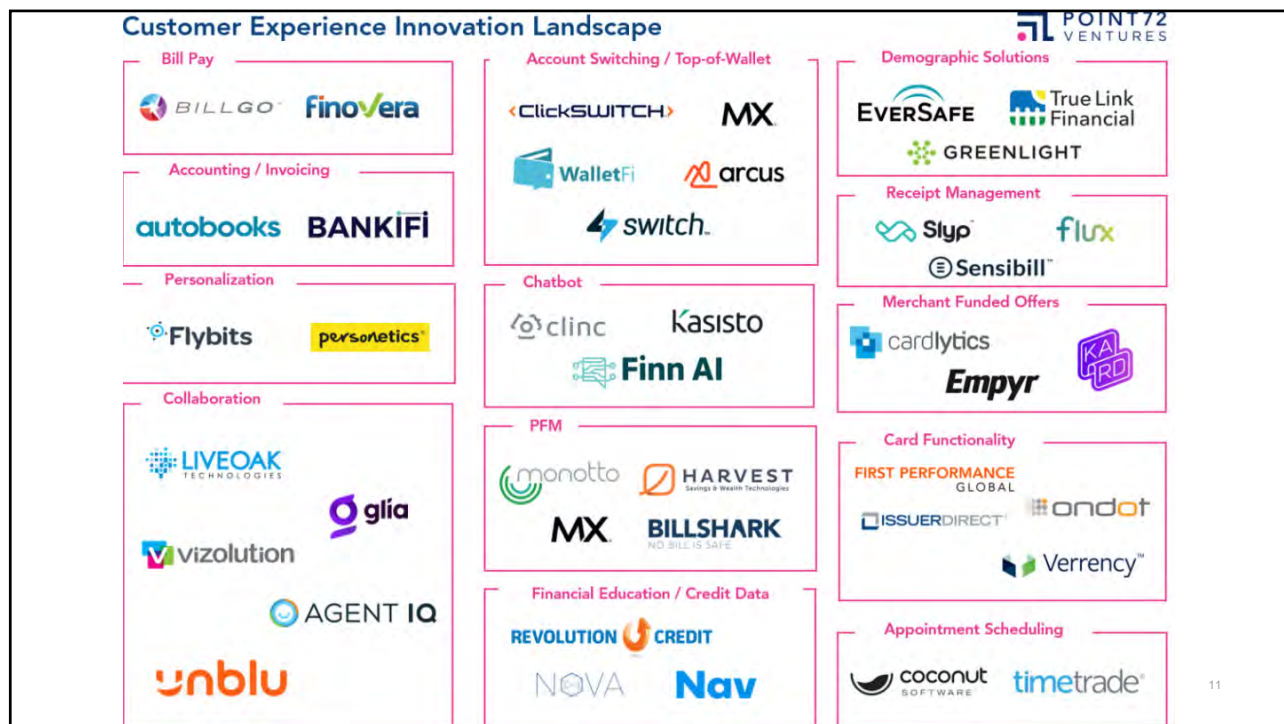
2018 and Beyond: Hybrid Strategy

- Innovation arm working in collaboration with FinTech to launch products in the market
- Investment arm working on investment and acquisition
- Open banking app-store model

9

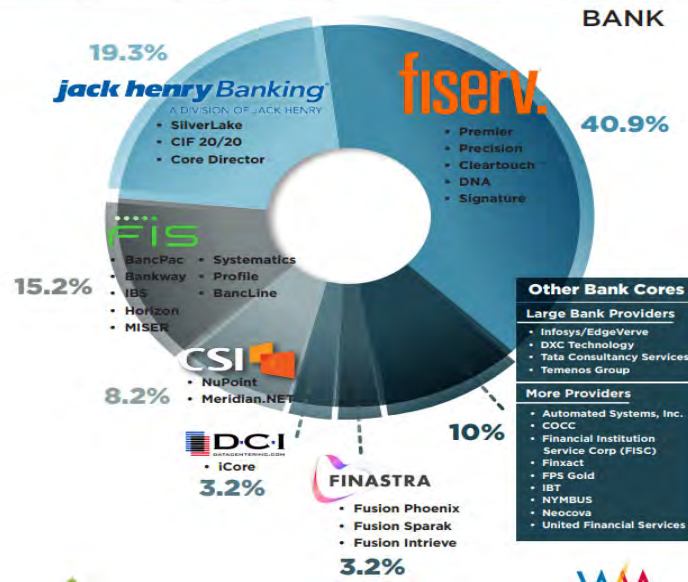


10



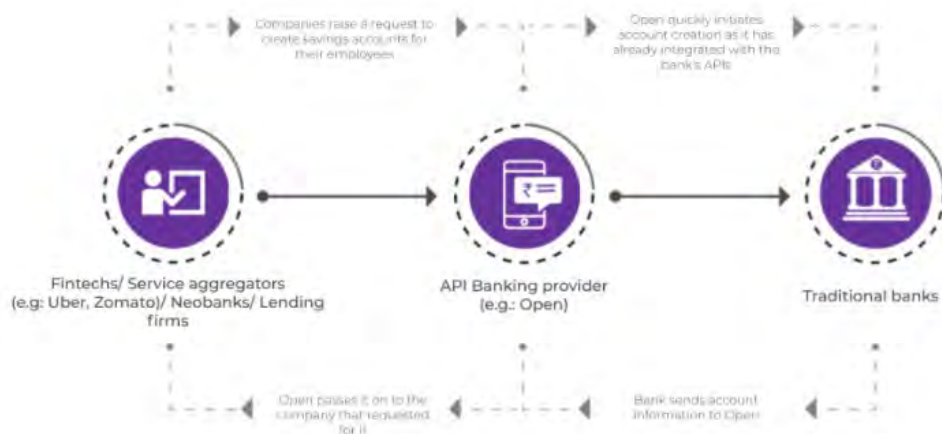
Core Market Leaders

U.S. Installs 2020



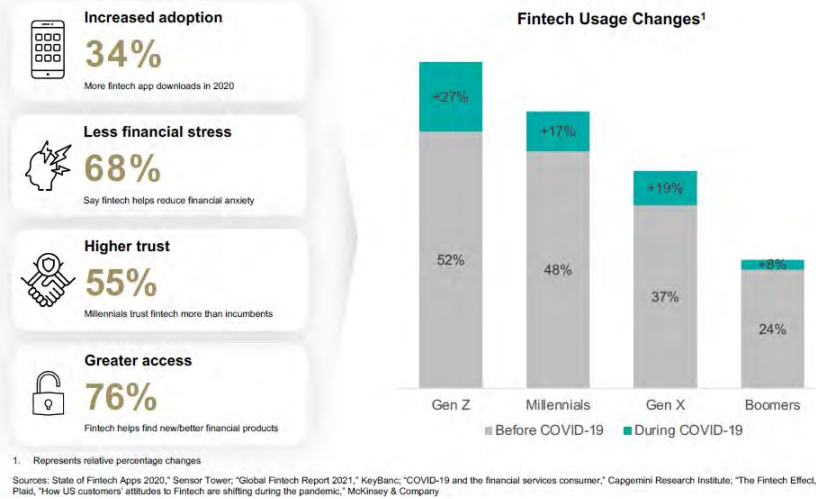
13

API's - How Banks and Fintechs/Brands connect



14

Fintech has redefined consumer expectations, COVID-19 forever shifted consumer engagement...



FinTech trends - startups and investment

- Lending – PON lending, RPA/Chatbots
- Security – Access management, education, fraud detection
- Small business - payments, ledger, cash management
- Financial wellness – education, charitable giving
- Data analytics – regulatory reporting, customer profitability, marketing
- Marketing – geo location, affiliate marketing
- Core enhancement – dumb core with app store in front

WIPFLI

FinTech from the investors view

Venture capital

- Alternative lending
- Capital markets
- Consumer finance
- Digital assets
- InsureTech
- Money transfer
- Payments
- RegTech
- WealthTech

Community banks

- Consumer finance
- Money transfer
- Payments
- Digital onboarding
- Digital first core
- Real time payments
- SMB services
- Data management/services

17

Banking as a service business model

- Small and regional banks providing the banking services for FinTechs and other brands
- Banks receive fee income and cheap deposits
- FinTechs own the customer and tech
- Banks need technology and compliance expertise
- Chime is an example but there are many

Banking as a service

- What is it?
 - ▶ FinTech or another brand
 - ▶ Embedded: app-based deposit, loan or payment product
 - ▶ The product sits on (or off) the bank's balance sheet
 - ▶ All connected by a special set of Application Processing Interfaces (APIs)


19

Banking as a service – example

- What is it?
 - ▶ FinTech or another brand
 - ▶ Embedded an app-based deposit, loan or payment product (mobile savings, debit cards, credit builder, early payments)
 - ▶ The product sits on the bank's balance sheet
 - ▶ All connected by a special set of Application processing interfaces



chime®



Chime is a financial technology company. Banking services provided by The Bancorp Bank or Stride Bank, N.A.; Members FDIC



COASTAL
COMMUNITY BANK®

- Based in Everett, WA
- Asset Size: \$2.1 Billion
- 22.1% Compound Annual Growth Rate in Assets since 2010
- Founded: 1997
- Employees: 250
- Website: coastalbank.com
- Eric Sprink, President and CEO

Case study

- Eric Sprink, President and CEO at Coastal Community Bank, based in Everett, Wash., oversees not one but three growing organizations.
 - One is the bank itself, an expanding community financial institution, with \$2 billion in assets,
 - Another is CCBX, a division of the bank that specializes in banking as a service deals with fintechs and neobanks
 - CCDB, the company's digital banking division. Its main task at present is preparing the bank to partner in the Google Plex family of products in 2021 or 2022.
- Coastal began looking at banking as a service in 2015, and has steadily grown its base of partners, with the pace picking up in latter 2020 and into 2021.
 - The bank has gone about the partnering process selectively, vetting over 900 potential BaaS partners.
 - 21 partners in stages of signed letters of intent, implementation/onboarding, "friends and family" operation, and fully active. Six of those partners came on in the first half of 2021.
- In 2020 Coastal booked BaaS fees of \$2.3 million, up nearly 15% over 2019 and second in fee income only to deposit service charges and fees. BaaS accounted for nearly 5% of deposits at the end of 2020.

©The Financial Brand – June 24, 2021



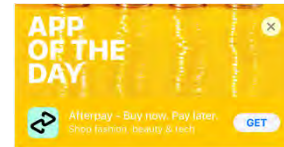
Coastal has a number TAM & Growth & Growth Partners & Partners Growth

“We don’t look for programmers. We’re looking for bankers who are able to work with our partners who happen to do things via technology.”

— Eric Sprink, Coastal Community Bank

Point of need financing

- What is it?
 - ▶ Allows “buyers” flexible loan terms
 - ▶ Delivered at time of purchase
 - ▶ Approval decisions are made programmatically
 - ▶ A modern version of indirect lending



Want to buy some clothes but don't want to pay for them all at once?

You have some flexibility thanks to Afterpay, a service that provides interest-free payment plans at nearly 3,000 retailers including Levi's, Free People, and DSW.

Here's how it works: Pull up the Afterpay app, browse through the member retailers, and find an item you love—the fabulous new wet-look eyeshadow or limited-edition sneaker drop. Alongside the price, you'll see that it's available in four payments via Afterpay. A retro Jordan release that retails at \$270, for example, is available for four installments of \$67.50.

Check out using Afterpay—an option clearly marked with most participating retailers—and you'll pay for it in four parts: one at the time of checkout and

25

Community bank point of need finance alternative



- Philadelphia based start-up
- Objective is to grow consumer customer portfolio
- Application based – phone or tablet
- FI's own underwriting criteria
- Fee income plus interest income
- Use cases
 - ▶ Home improvement loans
 - ▶ Solar
 - ▶ Elective Medical
 - ▶ RVs

26

Financial wellness/literacy/unbanked/underbanked

- Increased focus on financial wellness and unbanked/underbanked given the new administration
- Increasing trend of FinTech startups attempting to create solutions to address FW
- Age demographics seem to be driving the increased attention
- COVID has also focused attention on financial wellness

zogo

Plinqit

Banker Jr.

 **pocketnest.**

27

CHALLENGER BANKS' STRATEGY:

PRODUCT PERSONALIZATION



CORNERSTONE
ADVISORS

@rshevlm

The era of hyper-personalization

“there is an app for that”

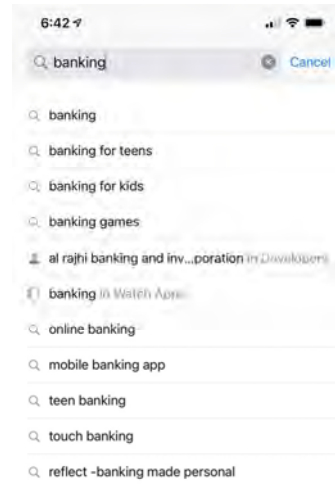
Banking as a function as opposed to a place to go

Enabling lifestyles

Serving lifecycle needs

Serving “communities” as opposed to “the community”

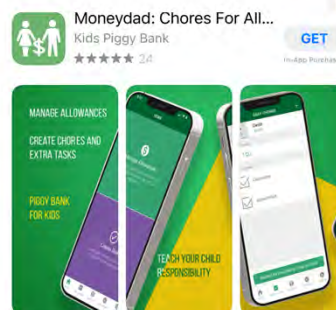
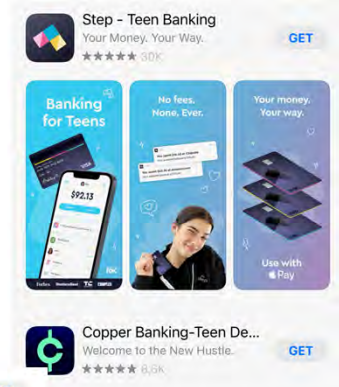
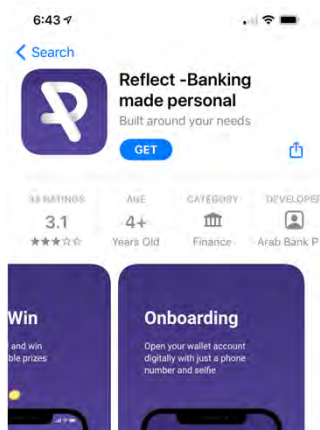
The app is backed by a bank or partners with a bank or bank account



29

The era of hyper-personalization

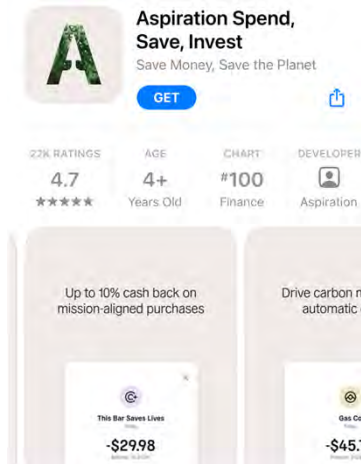
“there is an app for that”



30

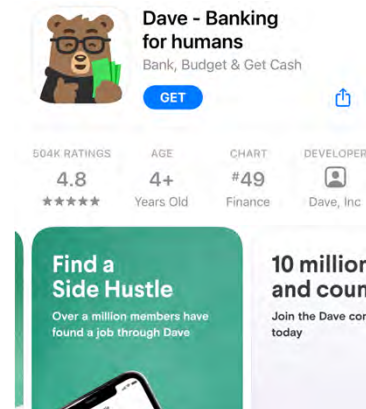
The era of hyper-personalization

“there is an app for that”



“Save Money,
Save the Planet”

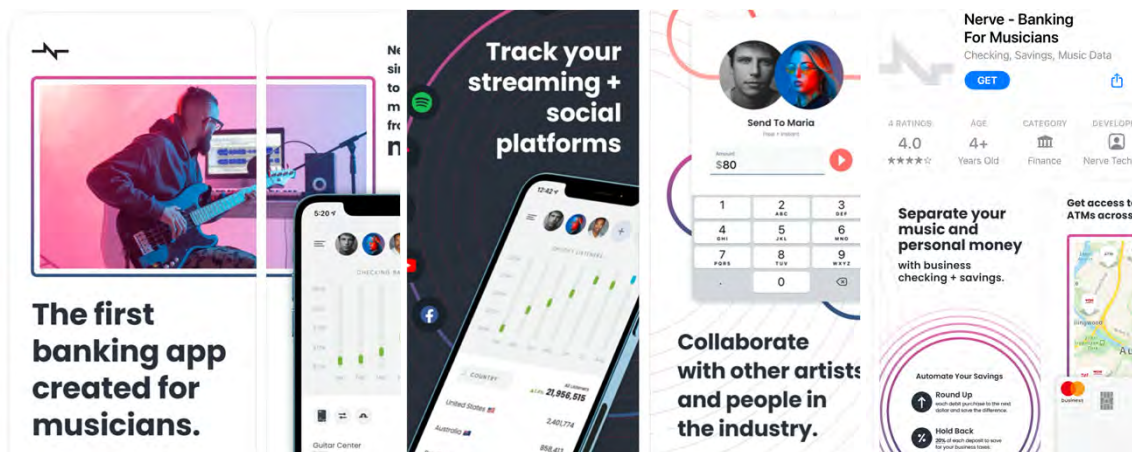
Banking app that helps you find a “gig” or job and manage cashflow, even a short-term loan.



31

The era of hyper-personalization

“there is a Bank for that”





Forecasting the future

“As computers become smarter, we no longer need humans as intermediaries. Professions whose basis is in transactions will be disrupted by machines – there is no question. And it will happen fast.”

- Amy Webb, founder of the Future Today Institute

“In all affairs it's a healthy thing now and then to hang a question mark on the things you have long taken for granted.”

- Bertrand Russell

“Silicon Valley is coming. There are hundreds of start ups with a lot of brains and money working on various alternatives to traditional banking.”

- Jamie Dimon in 2015 annual letter to shareholders of JPMorgan Chase

“Banking is necessary, banks are not.”

- Bill Gates in 1994

Innovation mindset – leaders

It's about the “AHA's”

- awareness, humility, and action

- Be **AWARE** of how technological, economic, social, cultural, and political trends are accelerating, burgeoning, and converging
- Have **HUMILITY** to the idea that what worked yesterday might not be sufficient tomorrow
- Take **ACTION** to create a new and better future

- Jack Uldrich, Business as Unusual

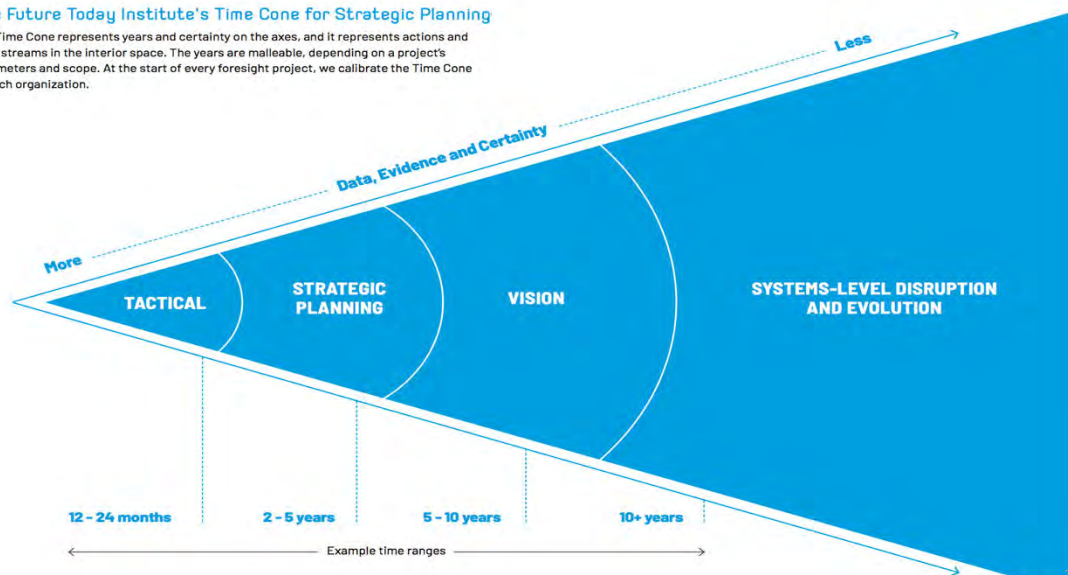
35

Innovation

how to do strategic planning like a Futurist

The Future Today Institute's Time Cone for Strategic Planning

The Time Cone represents years and certainty on the axes, and it represents actions and work streams in the interior space. The years are malleable, depending on a project's parameters and scope. At the start of every foresight project, we calibrate the Time Cone to each organization.



36

Forecasting the future

11 macro sources of disruption

1. Wealth Distribution – distribution, concentration, mobility
2. Education – access, quality, how, what tools, and interest
3. Infrastructure – physical, organizational, and digital
4. Government – planning cycles, and regulatory decisions
5. Geopolitics – leaders, militaries, and governments
6. Economy – shifts in macro and microeconomic factors

Source: The Future Today Institute

Forecasting the future

11 macro sources of disruption

7. Public Health – lifestyles, pop culture, disease, govt regulation, warfare or conflict, religious beliefs
8. Demographics – dynamics shifting communities
9. Environment – natural world, including extreme events
10. Media and Telecommunications – ways in which we send and receive information and learn about the world
11. Technology – connective tissue linking business, govt and society

Source: The Future Today Institute



Futurist View of Financial Technology

Futurist view of financial technology

Tech companies acting like banks:

Alibaba, Amazon, Ant Financial, Apple, Citi, Chase, Goldman, Google Square, Stripe, etc.

Impact: big tech have made payments easier and this will put pressure on traditional banking – disrupting consumer and smb.

Futurist view of financial technology

Financial inclusion:

Lack of financial education will continue to be a barrier for people, excluding them from financial services and systems.

Digital and mobile payments continue to grow with promising programs that leverage crypto currencies for remittances and humanitarian aid.

Source: The Future Today Institute

41

Futurist view of financial technology

The rise of Quant Funds:

Quantitative hedge funds have been around since the 1990s. These are algorithm-powered funds that follow factors set by humans, and they're taking over more of the US stock market.

Regulating open banking:

The EU and UK passed laws requiring open API for third-party developers. New standard will make it easier for vendor integration, compliance, reporting, and data management.

Source: The Future Today Institute

42

Futurist view of financial technology

Social payments:

Financial service and payment providers are tapping into social interactions to facilitate financial transactions. As social offerings grow more robust, millennials/Gen Z may opt out of traditional banking services entirely. This includes smb.

Countries creating digital decentralized currencies:

Examples are China and Sweden – according to a report from the Bank of International Settlements, 80% of the 63 central banks surveyed are researching whether and when to release their own digital/crypto currencies.

Source: The Future Today Institute

43

Futurist view of financial technology

Automated credit risk modeling:

Using artificial intelligence, machine learning, and robotic process automation to create models and processes for all types of lending.

Crypto trading bots:

Monitor the market 24/7 since the crypto markets never close. Send instructions to the bot and it will carry out its commands (still is glitchy)

Source: The Future Today Institute

44

Questions



Marcie Bomberg - Montoya

Principal

708 522 7161

marcie.bomberg@wipfli.com

© 2022 Wipfli LLP. All rights reserved.
"Wipfli" refers to Wipfli LLP.

WIPFLI

1:40 – 2:30 p.m.

Prepare Now to Accelerate Your Business With Instant Payments & the FedNow Service

Tim Boike, *Vice President of Industry Relations & Engagement,
Federal Reserve Bank of Chicago*

Ready, Set, FedNow: Accelerate Your Business with Instant Payments

Wisconsin Institute of Certified Public Accountants
Brookfield, WI
May 10, 2022

©2022 Federal Reserve Banks. Materials are not to be used without consent

NONCONFIDENTIAL // EXTERNAL

Federal Reserve research

Retail Payments Study / Survey Consumer Payment Choice

Demand for instant payments are growing in the United States due to a culture of on-demand services, transparency and fulfillment.



In 2019, 59% of consumers adopted mobile banking and 75% online banking.



The growth rate of noncash payments was 6.7% per year from 2015 to 2018.



In 2019, half of consumers adopted at least one online faster payment method.



Between 2015 and 2018, checks declined at a compound annual rate of more than 7%.



Electronic payment methods linked to a bank account are used for more than 40% of bill payments by consumers.

Sources: 2019 Federal Reserve Retail Payments Study, 2019 Survey of Consumer Payment Choice, 2019 Diary of Consumer Payment Choice

Federal Reserve research

Faster Payments Market Readiness Brief

The Federal Reserve published results of a survey of 2,010 businesses to assess their current payment practices as well as their potential usage and expected benefits of faster payments.



Industry categories

- 44% work for service businesses
- 36% work for either manufacturing or retail businesses
- 20% work in the wholesale segment or other categories



Business sizes Based on annual revenue

- 32% were from large/very large businesses
- 68% were evenly split between medium-sized, small and micro businesses

The sample of 2,010 allows for a sampling margin of error of +/- 4% at a 95% confidence level.

Source: FedPayments Improvement, *Market Readiness Brief: Businesses look to the future with faster payments*, August 2021



©2022 Federal Reserve Banks. Materials are not to be used without consent

THE FEDERAL RESERVE
Financial Services

3

Federal Reserve research

Faster Payments Market Readiness Brief



A majority of surveyed businesses consider it important to use faster payments. Nearly two-thirds indicated they would factor access to faster payments into **future decisions on whether to switch banks**.



Businesses want to use faster payments for **quicker access to funds and the ability to post immediately / automatically**. They also want immediate notification of payment and remittance details with the payment.



Nine in 10 businesses expect to be able to **initiate and receive faster payments by 2023**; many are ready to do so now.



A majority of the businesses surveyed have **already sent and received some type of faster payment in the past 12 months**, using primarily digital wallets, Same Day ACH and push-to-card.



Use cases of greatest interest to businesses include **e-invoicing and bill pay with remittance details**. These require data and messaging capabilities that instant payment options are well positioned to support.



©2022 Federal Reserve Banks. Materials are not to be used without consent

THE FEDERAL RESERVE
Financial Services

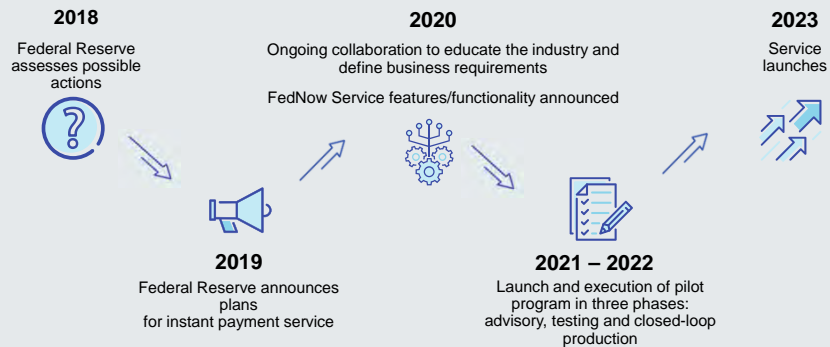
4

Pandemic's impact on faster payment adoption

The pandemic has had a significant impact on the financial operations of the businesses the Federal Reserve surveyed.



From inquiry to innovation



The FedNow Service

The FedNow Service is a way for financial institutions of every size and in every U.S. community to provide safe and efficient instant payment services around the clock, 365 days a year.

Delivers real-time gross settlement of funds, with integrated clearing functionality, 24x7x365

Enables funds transfers, settlement and confirmation of good funds in real time



Offered to all financial institutions to enable businesses and individuals to send and receive instant payments conveniently

Supports a range of use cases

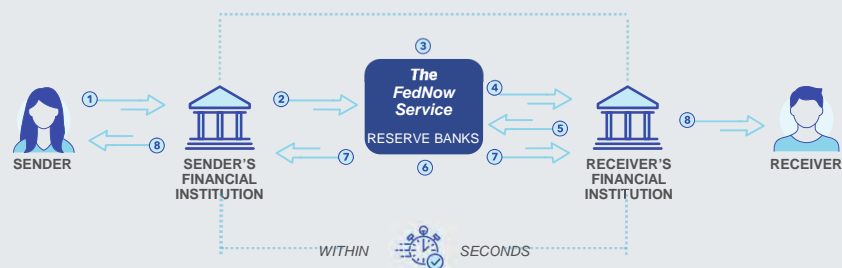


©2022 Federal Reserve Banks. Materials are not to be used without consent

THE FEDERAL RESERVE
Financial Services

7

The FedNow Service payment flow



©2022 Federal Reserve Banks. Materials are not to be used without consent

THE FEDERAL RESERVE
Financial Services

8

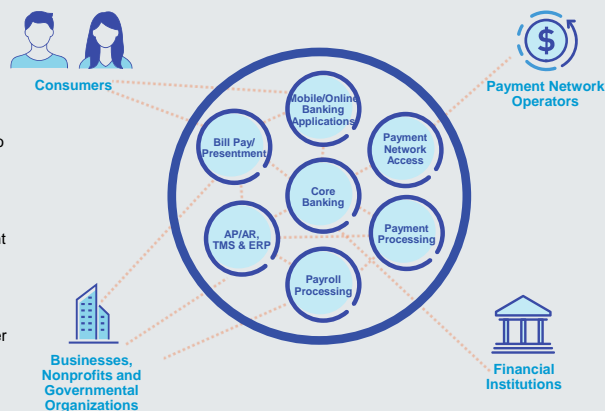
The FedNow Service in action

Follow a payment over the FedNow Service from start to finish and see what financial institutions should know about their role in the process.



Collaboration across the entire ecosystem

- Financial institutions**
 Financial institutions can connect directly to the FedNow Service or through their service provider.
- Payment service providers**
 Service providers can connect directly into the FedNow Service on behalf of a FedNow participant/financial institution.
- End users**
 End users can enjoy the benefits of instant payments offered by their financial institutions.
- Other industry providers**
 Other industry providers can work together with financial institutions to create and offer a variety of instant payment solutions.



The FedNow Service is Use Case Agnostic



CONSUMER-TO-BUSINESS (C2B)

- Individual to a business
- Groceries, haircuts, gym memberships, etc.
 - Bill payments



ACCOUNT-TO-ACCOUNT (A2A)

- Funds transfer from one customer's account to another account owned by the same customer
- Transferring funds from a bank account to a brokerage account



CONSUMER-TO-GOVT (C2G)

- Individual to a government entity
- Taxes or federal fees for park passes, licenses, etc.



BUSINESS-TO-CONSUMER (B2C)

- Business to a person
- Rebates, wages, etc.



PERSON-TO-PERSON (P2P)

- Individuals to friends, family, other individuals
- Babysitting, rent, utilities, meals, etc.



BUSINESS-TO-BUSINESS (B2B)

- One business to another
- To suppliers for inventory, rent, services, etc.



BUSINESS-TO-GOVT (B2G)

- Business to a government entity
- Federal or state tax payments



GOVT-TO-CONSUMER (G2C)

- Government to an individual
- Tax refunds, social security benefits, etc.



©2022 Federal Reserve Banks. Materials are not to be used without consent

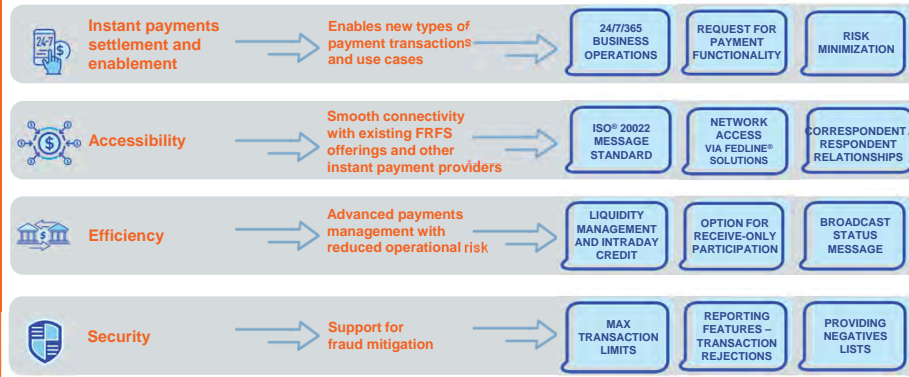


11

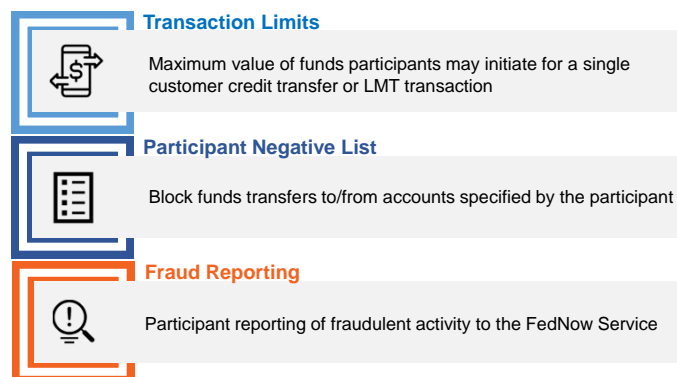
FedNowSM Service
functionality

©2022 Federal Reserve Banks. Materials are not to be used without consent

Building to our public mission and industry needs



Fraud prevention features at launch



Liquidity management transfers (LMT)



LMT value limit

- Per-transaction value limit between \$2.5 million and \$5 million



LMT hours of availability







Hours under consideration are weekdays 7 p.m. – 7 a.m. ET and 24 hours per day on weekends and holidays



LMT fee

LMT per transfer fee will be higher than the highest Fedwire Funds Service per transfer fee (currently \$0.88)

Available Reports

FedNow Reports	 Account Balance	 Activity Totals <i>summary level</i>	 Activity Details <i>detail level</i>
	 Daily Statement of Account <i>summary level</i>	 Financial Institution Reconciliation Data (FIRD) <i>detail level</i>	 Statement of Account in Spreadsheet Format (SASF) <i>detail level</i>

7-Day Accounting

The Federal Reserve will operate under a 7-day Accounting Cycle upon the implementation of the FedNow Service



Opening/Closing Balance Calculations

Balances will be calculated 7 days a week at the end of each Accounting cycle day.



FedNow/Accounting Cycle Date Rollover

FedNow Service close of cycle will align with the Fedwire® Funds Service end-of-day close at 7:00 p.m. ET.

Accounting end-of-day cycle at approximately 8:00 p.m. ET.



Balance Inquiries

Real-time balance inquiry reports will be available via the FedNow Service and the Account Management Information (AMI) application.



Correspondent/Respondent Relationships

Correspondent/Respondent relationships can be established by completing the Operating Circular 1 (OC 1), Appendix 2 (Transaction and Service Fee Settlement Form).

Non-account holders must designate a correspondent to settle FedNow transactions.

Master Accounts can designate a correspondent, if desired.



©2022 Federal Reserve Banks. Materials are not to be used without consent

THE FEDERAL RESERVE
Financial Services

17

Reconciliation Overview

While operating 24x7x365, the FedNow Service will declare a closing time for each processing date, to enable reconciliation.



Types of Reconciliation

- Reconciling against debit/credit totals posted to Federal Reserve master accounts
- Reconciling with Customers' accounts

Reconciliation Tools

- New FedNow Service specific Reports
- Existing Accounting Reports



©2022 Federal Reserve Banks. Materials are not to be used without consent

THE FEDERAL RESERVE
Financial Services

18

Cycle Date

Fedwire Funds Service /FedNow Service Cycle Date Close (7:00 pm ET)

Represents the end of the processing day for the FedNow Service, in alignment with Fedwire Funds Service

Accounting End-of-Day (EOD) Cycle (~8:00 pm ET)

Timing for when Federal Reserve Accounting has received all debit and credit transactions posting to an institution's account from all business lines within the Federal Reserve, to determine the institution's closing balance for the given cycle date

Provisional Balance

A provisional balance is provided when FedNow Service/Fedwire Funds Service have rolled into the new cycle day, but before Federal Reserve Accounting has completed its end of day cycle process



©2022 Federal Reserve Banks. Materials are not to be used without consent

THE FEDERAL RESERVE
Financial Services

19

FedNow Progress

©2022 Federal Reserve Banks. Materials are not to be used without consent

Pilot program: Industry input and collaboration



More than 120 organizations are contributing to the development, testing and adoption of the FedNow Service. Learnings and activities from the program will inform the product build.

Advisory:

- Further define the service and outline an adoption roadmap
- Develop industry readiness approaches and overall strategy

Testing:

- Perform test cases and provide feedback
- Identify issues for remediation

Closed Production:

- Send live transactions to other participants
- Participate in resiliency testing
- Validate the end-to-end payments flow

FedNow Pilot Program progress



What's next in the pilot?



Continuing the advisory phase:

- Additional content and deep dives
- Feedback will continue to shape product features, readiness activities and education needs



Preparing participants for the testing phase:

- Onboarding Managers assigned
- "Discovery" sessions
- Technical deep dives
- Onboarding activities



Evolving the program:

- Continued engagement to support FedNow Service roadmap development and testing of future releases

Anticipated price points



\$25 Monthly Fee

Paid per RTN enrolled in the FedNow Service to receive transactions



4.5c Credit Transfer Fee

Paid by sender of the instruction



1c Request for Payment Fee

Paid by sender of the RFP

FedNow Service transfer value limit



- Credit transfer transaction value limit will be set at \$500,000
- Default value limit for participants set at \$100,000, with the option to adjust up or down
- Continue to evaluate the value limit on an ongoing basis and adjust as appropriate

Preparation & Readiness

The FedNow Community

Purpose:

Over **2,000 industry leaders**, representing more than **1,000 organizations**, have an opportunity to inform and evolve the development of the FedNow Service.

Engagement opportunities:

- Focus groups
- Working groups
- Surveys
- 1:1 conversations

Benefits:

- Exclusive invitations to events, first-to-know member communications on FedNow progress and engagement opportunities

Get involved:

- Join via FRBservices.org: Financial Services tab ➤ FedNow Service ➤ FedNow Community ➤ "Join the Community" button ➤ Complete questionnaire ➤ Submit



©2022 Federal Reserve Banks. Materials are not to be used without consent

THE FEDERAL RESERVE
Financial Services

27

How organizations can prepare

Preparation and planning is the best way to make a more seamless transition to the FedNow Service.

Questions for your organization to consider include:



What additional capabilities, if any, will be needed to handle real-time processing?



Are systems set up to alert customers of payments received or other status messages and to meet anticipated requirements to make funds available immediately?



What customer experiences and functionality are desired?



What areas have security and resiliency implications to support around-the-clock activity?



What data capabilities will be needed for customers and internal needs? Participants should consider how they will manage data needs.

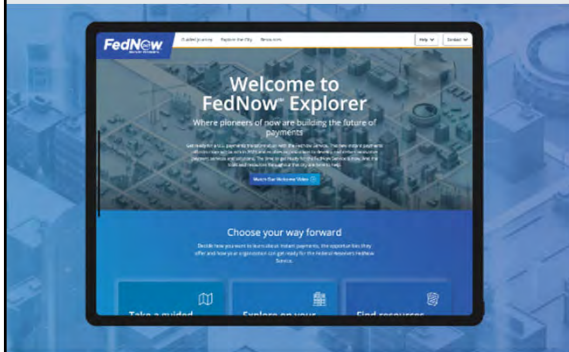


©2022 Federal Reserve Banks. Materials are not to be used without consent

THE FEDERAL RESERVE
Financial Services

28

FedNow Explorer

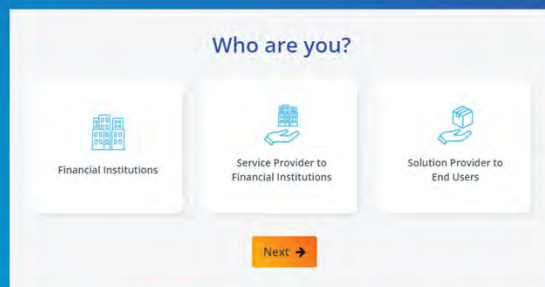


An experiential platform designed to educate and engage financial institutions and service providers

- Find curated content and business tools to support your instant payments journey
- Visit FedNowExplorer.org

Take a guided journey

Answer a few simple questions about your organization and we'll take you through a guided learning journey to get you up to speed on everything you need to know about instant payments, including how to prepare for the launch of the FedNowSM Service.

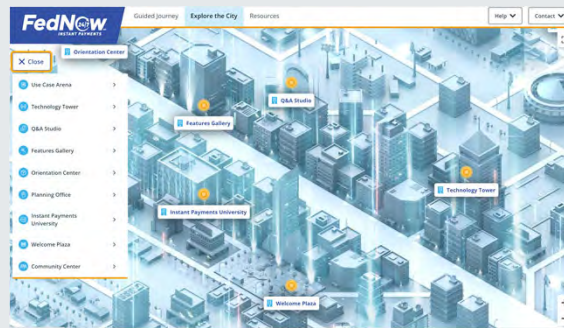


Unsure where to begin?

Explorer can guide you through the platform's content by answering a few questions

Explore on your own

Explore the city to find tools and resources on a variety of topics related to instant payments, use cases, product features and preparing for implementation of the FedNow Service



Preplanning Roadmap

Review the key steps to take on your path to a 24x7x365 instant payments world



The FedNow Service Readiness Guide

- Planning considerations for product, technology and treasury operations
- Operational details and benefits related to reporting and reconciliation, settlement and liquidity management
- Technology overviews regarding information security, participant availability and more

Welcome to the FedNow Service Readiness Guide

The Federal Reserve Banks are designing the FedNow Service, a safe and efficient instant payments infrastructure that will help modernize the U.S. payments system.

Financial institutions of all sizes across the United States that are eligible for Federal Reserve Financial Services will be able to use the FedNow Service to enable their customers to instantly send and receive money any time of day, any day of the year.

With the FedNow Service, financial institutions, their service providers and others in the payments industry can unlock a range of innovative instant payment use cases that offer benefits all around.



FINANCIAL INSTITUTIONS
Remain competitive, create new products and meet the needs of customers.



INDIVIDUALS
Instantly send and receive money with confidence and reduce the risk of overdraft and late fees.







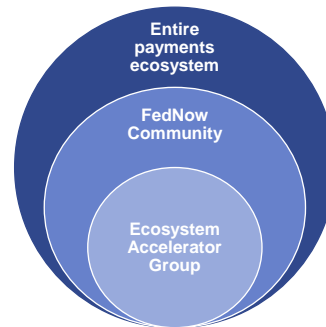
BUSINESSES
Gain better control of cash flow, manage, improve efficiency of corporate payments and streamline reconciliation processes.

We invite you to start preparing now for the FedNow Service. And this guide is here to help.

What is the Ecosystem Accelerator Group?

An interest group within the FedNow Community that will enable payment service providers across the industry to:

-  Influence FedNow Service design and release priorities
-  Participate in programs designed for the needs and interests of solution developers and providers
-  Ask technical questions and obtain answers relevant to this ecosystem group
-  Network with the broader FedNow Community and potential partners among financial institutions, other service providers and business clients



Service Provider Showcase

- Launched in Q1 - 2022
- Partner enablement online platform
 - Service Providers seeking financial institutions and other partners
 - Financial Institutions seeking to connect with use case enabling service providers
- Inclusive of narrative profiles, optional video, and contact information of participating service providers



Service Provider Showcase

Strong level of industry interest

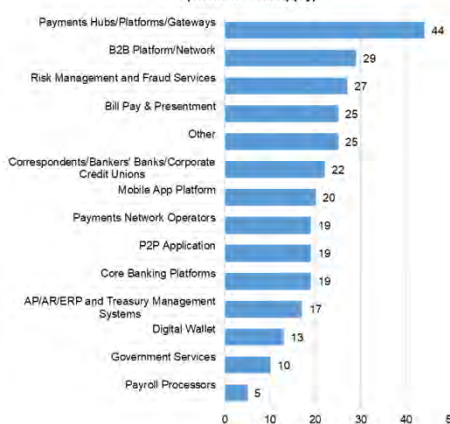


150+ attendees asked
20+ questions during the
January 2022 info session



Submissions from ~80 industry
organizations for launch, with more
citing participation in the coming
months

**Showcase Participants by
Segment/Solution Type**
(select all that apply)



tim.boike@chi.frb.org

(312) 322-5751

©2022 Federal Reserve Banks. Materials are not to be used without consent.

2:40 – 3:30 p.m.

Trends in Fraud & Financial Crime

Ben Brockman, CAMS, *Manager, RSM US LLP*

FINANCIAL CRIME AND FRAUD TRENDS

WICPA

May 2022

Speaker



Ben Brockman, CAMS

Manager, RSM US LLP

Ben works in RSM's anti-money laundering and regulatory compliance practice. He has over 14 years of experience working with financial institutions with a career-targeted focus specific to BSA/AML, and fraud. At RSM, he is responsible for leading the execution of AML, fraud and cryptocurrency engagements, including planning, coordination of fieldwork and delivery of client reports.

ELECTRONIC FUNDS TRANSFER (EFT) FRAUD

What are EFTs?

An electronic funds transfer (EFT) is the electronic transfer of money over an online network. They are a part of our daily lives due to their ease and speed. Here are some of the most popular EFT services in the US:

- Zelle – Used for peer-to-peer payments or to registered businesses. Owned by seven of U.S. largest banks (BoA, BB&T, Capital One, JPMorgan Chase, PNC, U.S. Bank, and Wells Fargo). Linked directly into your bank account which increases payment speed, which is convenient, but also means fraudulent payments happen instantly.
- Venmo – used for peer-to-peer as well as to verified business. Owned by Paypal and links to debit or credit card for payments. Funds are held in cloud and can be accessed by Venmo Debit card until deposited into an account.
- Cashapp – peer-to-peer payment service owned by Square Inc. Allows investing and early paycheck access. Allows customers to use a physical cash card for ATM withdrawals. Links to debit card for deposits into bank accounts.



EFT Fraud



As the use of EFTs has increased, the opportunities for scammers and fraudsters to steal money has increased as well. Within this area, scams usually fall into two groups:

- Phishing/Account takeover through stealing login information.
- Soliciting payments from verified users.

There is still a lot of discussion around who faces the monetary losses for these fraudulent activities. It differs for each scheme, but many banks and payment services claim zero responsibility due to customers authorizing these transactions. Who ultimately pays for the fraudulent activity depends on the transaction, bank fraud policies and payment service.

The next few slides we will discuss these scams further, and how they are being combatted.

Fraud
Someone gained **unauthorized** access to your money.

EXAMPLE
Someone gained access to your bank account without your permission. You never authorized or were involved in the transaction.

WHAT TO DO
Immediately report suspected unauthorized activity to your financial institution.

CAN YOU GET YOUR MONEY BACK?
Because you **did not authorize** a payment, you are typically able to get your money back.

EFT Phishing Scams



There are thousands of attempted EFT scams daily. The majority of these scams are phishing scams via text, email, and calls to get account information. Once the victim's login information is compromised, the scammer will send money to themselves. These scams may look like the following:

- *As you are a long-time user of Venmo, you have been selected to take a \$100 paid survey at this link.*
- *This is Zelle technical support, your account is suspended due to too many false password attempts. Please reset your password here with this link.*
- *PayPal Fraud Alert – Please sign in here to confirm identity.*

EFT services have begun to utilize Two-Factor Authentication, issued warnings of common schemes to their users, created fraud alert texts, and developed training sessions to help prevent phishing fraud.

Please see real examples of EFT phishing attempts on the next slide:

EFT Phishing Scams Examples



The screenshot displays two examples of EFT phishing scams. On the left, an email from Venmo to a user named @username. The email states that a \$100 payment has been received and that the funds will be held until a tracking number is provided within 24 hours. It includes a 'Reply' button and a 'Forward' button. On the right, a screenshot of a PayPal account verification page. The page title is '[Urgent] Account Verification Required - Mozilla Thunderbird'. The page content includes a 'PayPal' logo and a section titled 'We noticed some unusual activity'. It lists several account limitations and a 'Secure My Account' button. Below the email, there is a text message from +1 (415) 324-9890 that says 'Venmo Deposit Confirmation. \$100 please confirm needlealarm.com/ir29ZIP'.

EFT Request Scams



There are also several EFT scams which are more strait forward and are designed to trick victims into sending money to fraudsters account. These scams differ from phishing scams as they do not steal any private information or access the victim's account. These scams are popular on online marketplace, dating and social media sites where the victim cannot verify the scammer's identity.

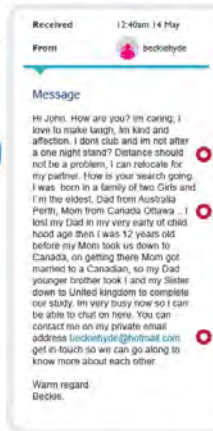
Three common examples of these are:

- *Online sellers of goods who are not registered businesses and are requesting payment via EFT prior to sending goods.*
- *Someone pretending to be a friend or relative and requesting money from you for emergency, typically targets elderly family members.*
- *Romance Scams – while more elaborate and take time, these scams will result with a request for money to "buy a ticket to see them."*

To combat these scams, online merchants have informed users on these tactics, bankers have been trained to identify these scams, and EFT services have created controls for verifying the phone number of EFT recipients prior to sending money.



EFT Request Scams



Acknowledges distance and offers to relocate on first contact

Story of growing up in Australia, Canada and completing study in the UK is surprising given the poor English

Provides email address and encourages use of that rather than continuing to chat within the dating web site.

Note the free cloud-based email address. Not unusual nowadays but be mindful that this person could be based anywhere in the world.



9

© 2022 RSM US LLP. All Rights Reserved.

COVID-19 & CARES ACT SCAMS AND FRAUD



CARES Act Fraud



The Coronavirus Aid, Relief, and Economic Security Act (CARES Act) was signed into law on March 27, 2020, for the purpose of aiding U.S. citizens and businesses during the Pandemic. Unfortunately, Fraudsters immediately found ways to manipulate and abuse the bill for their benefit.

In May 17, 2021, the Department of Justice established the COVID-19 Fraud Enforcement Task Force to combat and prevent pandemic-related fraud. Since its founding, the task force has charged over a hundred defendants with fraud surrounding to several aspects of coronavirus relief. These fraud schemes include the following:

- Stimulus Payment Fraud
- Unemployment Benefits Fraud
- SBA Loan Fraud including Paycheck Protection Program (PPP) loans and Economic Injury Disaster loans (EIDLs)
- Healthcare Benefits Fraud



Stimulus Payment Fraud



Throughout the past two years U.S citizens meeting specific criteria received up to three economic impact payment stimulus checks. Additionally, in 2021, eligible parents received monthly stimulus checks for up to \$300 per child (a policy which may reappear in 2022 through the Family Security Act). These payments were distributed either check or direct deposit if direct deposit was utilized on the individuals most recent tax return. Several fraud schemes have occurred within this area. See them below:

- Telephone scammers and robo-callers impersonating the IRS requesting information and requesting money from victims. These schemes may reference either real (economic impact payments) or fake (federal student tax) payments and taxes to trick victims into thinking they owe the IRS money and paying them.
- Fake letters from the scammers claiming to be the IRS demanding payments to locations/businesses that are not the IRS.
- Phishing and malware via text and email to trick taxpayers into thinking these are official communications from the IRS. These schemes typically target taxpayers to input personal information, such as SSN, DOB, address which scammers then use for more elaborate schemes.
- The most common phishing scam seen was the "Update your IRS e-file" scam which brought victims to a website identical to the IRS's site and made victims complete forms collecting their PII.



Stimulus Fraud Examples



COVID-19 Relief Update
12/22/2020: Congress has passed a 900 billion USD government stimulus package for COVID relief. What is in it for you Tim?

Tim, you are receiving this message because your tax records indicate annual earnings less than \$75,000 and are thus able to receive a Federal Stimulus Check to the sum of \$600,00 plus an unemployment benefit of \$300 for 11 weeks. Access benefits here: h01bstf.com/G88Sw up to \$20 000 per household

From: Customer Service <h01bstf.com/G88Sw>
Sent: Tuesday, August 24, 2021
To: Tim
Subject: Notification - For security reasons, please re-enter the correct banking data previously provided to the IRS.

IRS
Third Round of Economic Impact Payments Status Available

Dear Customer (IRS)

After the last annual calculation of your fiscal activity we have determined that you are eligible to receive a payment of \$15.00.

Each week and by sending the third payments to eligible individuals as we continue to process tax returns. Payments are sent by direct deposit to that as a credit to their card.

[Claim my payment](#)

Note: For security reasons, we will record your guidelines, the date and time. (Indicates using inputs are ultimately pursued and indicated.)

Sincerely,
[Signature]

U.S. TREASURY CHECK SECURITY FEATURES

Treasury Seal
The new seal reflecting "Bureau of the Fiscal Service" has replaced the old one. The old seal, reflecting "Financial Management Service" will be seen in rotation until this check stock runs out.

Shining Ink
The Treasury seal, located to the right of the Statue of Liberty, contains security ink that will run and turn red when moisture is applied to the black ink of the seal.

Microprinting
Microprinted words are so small they appear as just a line to the naked eye. However, when magnified, they become readable. Microprinting cannot be replicated by a copier and when a check is counterfeited, it will often show up as a solid line or a series of dots. The U.S. Treasury check has one area on the back where microprinting is used with the words "USAUSAUSAUSA".

Watermark
All U.S. Treasury checks are printed on watermarked paper. The watermark reads "U.S. TREASURY" and can be seen from both the front and back of the check when held up to a light. The watermark is light and cannot be reproduced by a copier. Any check not having the watermark should be suspected as being counterfeit or copied.

Ultraviolet Overprinting
A protective ultraviolet pattern, invisible to the naked eye, consisting of four lines of "FMS" located by the FMS seal on the left and the United States seal (right) on the right. This pattern can usually be found under the paper information and dollar amount area. The FMS pattern and words can be detected under a black light. If the amount box is shaded or altered in any way, a space will be created in the ultraviolet area. When exposed to black light, the ink used in the pattern and the seal will glow. This fluorescent quality cannot be photocopied.

As of October 2012, a new ultraviolet pattern was introduced into the check stock consisting of four lines of "FISCAL SERVICE" (see below). Also, the seal has been changed to read "Bureau of the Fiscal Service". Either one of these ultraviolet patterns may be seen until the prior check stock runs out.

Unemployment Benefits Fraud



Unemployment benefits fraud is a form of identity theft and has been one of the most popular schemes throughout the pandemic, accounting for over \$1 billion of fraudulent benefits payments from July 2020 – June 2021. Most victims of this scheme are not aware they are a victim until either alerted by the IRS or their employer. The process follows these steps:

- Fraudster accesses victim's PII (either through phishing scheme, purchasing from the dark web, etc.)
- Fraudster applies for unemployment as the victim and sends the unemployment checks to themselves.
- Victim is either alerted via their employer or by the IRS upon receipt of a form 1099-G.
- Victim reports fraud to the IRS and the payments are stopped.

Luckily, victims of this scheme will not owe taxes on these fraudulent funds if they follow all necessary steps to report the fraud to the IRS, but victims will know that their PII has been compromised. The DOJ has also warned of fraudsters creating fake unemployment benefit and state workforce agency sites to trick people into entering PII which can be used for identity theft.



How to Identify Unemployment Fraud



New York State
Department of Labor
PD 807 15.159
ALBANY NY 12212-5130

Unemployment Insurance
Notice of Potential Charges
Part 1 of 2

Date Mailed: 08/02/2020
Employee: [REDACTED]
Client: [REDACTED]

Use block or blue ink for corrections and/or updates to this notice.

If the above address is incorrect, refer to the reverse side of this notice for assistance.

Reason for this Notice: The claimant designated below has filed a claim for Unemployment Insurance benefits, naming you as a former employer. Please review the information below and follow the instructions for submitting an appeal. For

PREVENTING UNEMPLOYMENT FRAUD

FOR FRAUD VICTIMS

- Have your employer deny the claim.
- Call the IDES hotline at (800) 894-0513 to report the fraud OR see https://www2.illinois.gov/ides/Pages/Reporting-Unemployment_Insurance_Fraud.aspx
- If you receive an unemployment letter or a debit card from Keybank, do NOT activate the card. Destroy the card.
- Report the fraud attempt to the credit rating agencies. <https://www.consumer.ftc.gov/articles/0275-place-fraud-alert?%E2%80%8B#How>
- Sign up for free credit monitoring <https://www.annualcreditreport.com/index.action>

IDES is giving some priority to fraud victims, but call backs are slow. Our office is available to help in extenuating circumstances at 217-774-1306.

FOR EMPLOYERS

- Deny claims you know to be fraudulent & forward the above instructions to impacted employees.
- Review information on the SIDES and SIDES E-Responder system <https://www2.illinois.gov/ides/IDES%20Forms%20and%20Publications/SIDES%20March%202018.pdf#search=SIDES>



15

© 2022 RSM US LLP. All Rights Reserved.

SBA Loan Fraud



Since the enactment of the CARES Act, over \$800 billion in loans have been provided by the government to aid small businesses. This has led to an increase in both fraudulent applications (estimates of 15% of false loans accounting for \$76 billion in fraudulent activity) and scammers targeting small business owners with false loan information/opportunities to steal PII.

Regarding loan forgiveness, the SBA partnered with financial institutions to process PPP loans and disperse funds to borrowers, with then reimbursed lenders for each loan processed. Lenders were responsible for performing a good faith review of all loan applications which involved collecting all required documents (payroll reports, tax forms, IDs, etc.) and providing the information and loan calculation to the SBA. The SBA has identified hundreds of false loans during their audit of these loans and expects to uncover hundreds more.

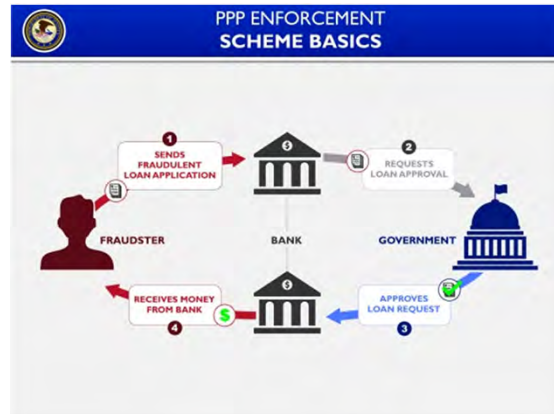
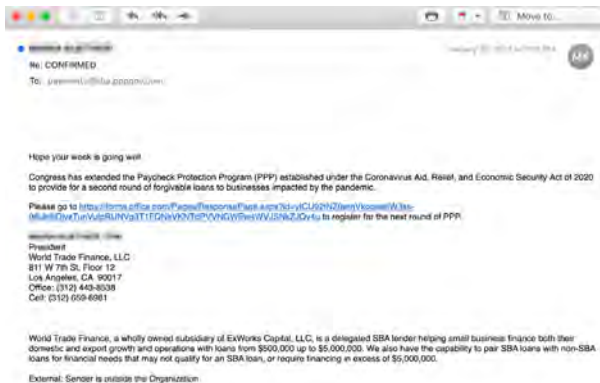
Outside of applying for fraudulent loans, fraudsters have begun contacting small businesses via email or phone to steal PII and either apply for PPP loans dispersed to them or use this PII for other identity theft schemes. Phishing schemes have greatly increased since the pandemic and coronavirus aid has been one of the most popular routes taken in these schemes.



16

© 2022 RSM US LLP. All Rights Reserved.

SBA Loan Fraud



17

© 2022 RSM US LLP. All Rights Reserved.

Healthcare Benefits Fraud



Outside of lending, fraudsters have utilized new healthcare policies for several schemes. These schemes are targeting both government funds and consumers for gaining illicit funds.

Government funding schemes include offering false tests/vaccines and running unauthorized expensive tests on Medicare beneficiaries for Medicare claims.

Schemes on consumers involve:

- Selling false covid tests, vaccine and protective gear that is not approved by the FDA.
- False vaccine/testing sites which collect PII to then utilize for other scams.
- Phishing texts, emails and calls regarding COVID testing to receive PII.



18

© 2022 RSM US LLP. All Rights Reserved.

Healthcare Benefits Fraud (continued)



Don't Let COVID-19 Infect You With Insurance Fraud

TOP 5 COVID-19 SCAMS

- 1 Fake "corona" insurance**
Watch for fake health insurance agents selling low-priced insurance to cover expensive treatment. Scammers may try to sell low-cost "corona insurance" or health policies that claim to have a coverage provision. Simply hang up on robocalls.
- 2 Cancelled health insurance**
Beware of bogus calls warning you that your health insurance was "cancelled." You may be given a toll-free line to call, or urged to click a link that installs malware. Most of these are attempts to steal your personal information.
- 3 Corona medicines, tests**
Scammers are peddling fake vaccines, drugs, "all-natural" or "organic" medicines — all "insured and paid for" by your health policy. But the novel coronavirus is exactly that — new — and there is no known cure yet.
- 4 Senior scams**
Beware of free virus "tests" at senior centers, health fairs or in your home. Scammers might ask for your Medicare number, SSN and other information to steal your medical identity. Talk to your doctor if you need a test. Call your insurer directly to answer your coverage questions.
- 5 Bogus travel insurance**
Be wary of pitches for travel insurance that claim to cover coronavirus-related trip cancellations. Most standard travel insurance policies may not cover viral outbreaks or pandemics. Know what your policy does and doesn't cover.

 **Coalition Against Insurance Fraud** Prevent the spread of COVID-19 fraud and share this message.
Source: insurancefraud.org/Covid-19/Fox

COVID-19 SCAMS INCLUDE:

TELEPHONE FRAUD

- Calls from "hospital officials"
- Requests for payment to help relatives

PHISHING

- Emails from national or global health authorities
- Requests for personal information
- Payment requests
- Attachments or links which contain malware

COVID-19 FRAUD ALERT

INTERPOL

BE VIGILANT . BE SKEPTICAL . BE SAFE

2021 National COVID-19 Health Care Fraud TAKEDOWN BY THE NUMBERS

14	Defendants charged
7	Federal districts
50+	Medical providers received adverse administrative actions for involvement in the schemes
\$143	Million in false billings

Source: DOJ and HHS-OIG



DIGITAL ASSETS FRAUD

Digital Assets & Cryptocurrencies



What is a digital Asset?

A digital asset is anything that exists in a digital format and comes with the right to use. This includes any data, image, file, document, video, etc. that is owned digitally. This includes NFTs

What is a crypto currency?

A cryptocurrency, crypto-currency, or crypto is a digital currency designed to work as a medium of exchange through a computer network that is not reliant on any central authority, such as a government or bank, to uphold or maintain it. Each cryptocurrency is unique and impossible to counterfeit as its information is stored within the blockchain public ledger.



What is a Digital Asset?



Images



Video



Design Files



Documents



PDFs



Presentations



Marketing Collateral

Content Assets

What is an NFT?



Non-Fungible Tokens (NFTs) are digital assets which are “tokenized” to create a unique digital certificate of ownership on the blockchain. NFTs are artwork (music, videos, photos, etc.) no tangible form of their own. Because they are not tangible, the purchasing and selling of NFTs surrounds the rights of the artwork and not the physical art. Because the popularity of NFTs has grown so quickly in such a new space, there have been several fraud issues and risks.

Like the art market, the biggest fraud risk surround NFTs deals with their value. Because it is impossible to state the true value of an NFT, they are being sold for whatever someone is willing to pay for them, and the prices range from pennies to millions of dollars.

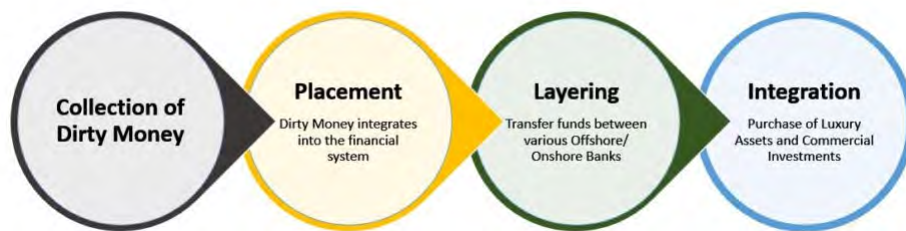


NFT Money Laundering



The subjective nature of NFTs has led to massive exposure to money laundering, especially since most NFTs are purchased with anonymous crypto currencies. The NFT money laundering process would generally follow these steps:

- You have \$X amount of illegal money. You use a third-party account to purchase crypto currency with this money.
- You create an NFT and list it for sale at \$X amount.
- You purchase your NFT from your third-party account and convert the crypto currency into USD citing that it was from the sale of digital art.



NFT Fraud



A popular fraud scheme within the NFT space are “rugpulls” which consist of a fraudster creating a fake NFT collection which they advertise and make false promises (such as the NFT will unlock certain features, triple in value, free future NFTs, etc.) only to run off once they have sold the fake collection. There are also several phishing scams and account access scams within this area to steal crypto currencies and NFTs from virtual wallets.

Since strong regulations, especially KYC regulations, on NFT exchanges has not been released yet, it is recommended that banks do not become involved in this activity. Updating KYC checklists/risk rating and screening for key words in transitions is the best first-line defense as we wait for solid regulations.



Cryptocurrency Fraud



Just like with NFTs, rugpulls are very common within the cryptocurrency market due to the volatile nature of most coins. A recent example of a rugpull dealt with \$SQUID coin which had no true ties to the Netflix show, Squid game, but jumped from one penny to above \$2,800.00 only to have the price free-fall to pennies minutes later. The scammer within this scheme earned over \$2 million with the victims suffering heavy losses.

Rug pull schemers generally recruit and pay social media influencers to promote the coin and spam online forums to raise the value of coins involved within these schemes. The SEC fined DJ Khaled and Floyd Mayweather for failing to disclose payments received for promoting an initial coin offering.

These schemes also work best with lesser known and cheaper currencies. Given the cost and popularity of common cryptocurrencies like Bitcoin and Ether, it is unlikely that schemers would target these currencies.

Cryptocurrency Fraud



25

© 2022 RSM US LLP. All Rights Reserved.

Cryptocurrency Fraud (continued)



Other common crypto related crimes include:

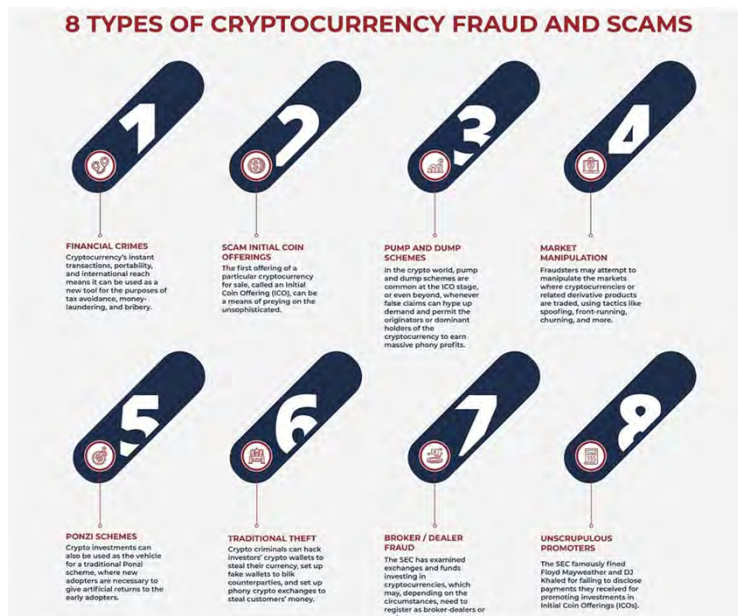
- Market manipulation such as spoofing, front running, and churning. This involves mass movements of currencies to inflate/deflate values of specific coins to influence trader's decisions.
- Initial Coin Offering (ICO) scams. ICOs are very similar to IPOs, but due to the lack of cryptocurrency regulations, these scams can leave potential investors handing over money for a fake coin.
- Virtual Wallet Theft. The crypto space is no stranger to hacking, phishing and other schemes to hack into victim's virtual wallets and liquidate their coins/NFTs into their own wallets.
- Traditional money laundering and terrorism proliferation through weak regulatory standards within this area.
- Stealth crypto mining which acts a trojan virus that takes over victim's computers and mines crypto currencies in the background while the victim is unaware.

In order to help protect customers from these schemes, banks should limit the coins and exchanges that customers can trade to help prevent customers from becoming fraud victims. Additionally, banks should increase KYC standards for customers engaging in this activity.

26

© 2022 RSM US LLP. All Rights Reserved.

Eight Popular Crypto Scams



RECENT TRENDS & CONCLUSION

Recent News – Canadian Emergencies Act



In February 2022, the Canadian Government invoked the Emergencies Act and expanded AML Rules to crowd funding sites and payment service providers (PSPs). Payment service providers are defined by the Retail Payments Activities Act as “an individual or entity that performs payment functions as a service or business activity that is not incidental to another service or business activity.”

Under the Emergencies Act, these entities were required to immediately cease the following activity for all designated persons participating in prohibited public assembly, entering Canada or traveling to an area with intent to participate in prohibited assembly, or facilitating assembly in any way:

- dealing in any property, wherever situated, that is owned, held or controlled, directly or indirectly, by a designated person or by a person acting on behalf of or at the direction of that designated person;
- facilitating any transaction related to the above;
- making available any property, including funds or virtual currency, to or for the benefit of a designated person or to a person acting on behalf of or at the direction of a designated person; or
- providing any financial or related services to or for the benefit of any designated person or acquire any such services from or for the benefit of any such person or entity.

Given that this was one of the first targeted regulations for payment services within the CFT area, we may expect expansion within US regulations to target domestic terror groups. Especially given that FinCEN stated targeting increase of domestic terrorism as one of its AML/CFT priorities within its June 30th, 2021, release.



Russian Sanctions & Evasion



Following Russia's invasion of Ukraine in February 2022, the United States Department of the Treasury released Directive 1A under Executive Order 14024 with the intent of, “Blocking property with respect to specified harmful foreign activities of the government of the Russian Federation.” This directive prohibits all U.S. financial institutions from the following activities:

- (1) as of June 14, 2021, participation in the primary market for ruble or non-ruble denominated bonds issued after June 14, 2021 by the Central Bank of the Russian Federation, the National Wealth Fund of the Russian Federation, or the Ministry of Finance of the Russian Federation;
- (2) as of June 14, 2021, lending ruble or non-ruble denominated funds to the Central Bank of the Russian Federation, the National Wealth Fund of the Russian Federation, or the Ministry of Finance of the Russian Federation; and
- (3) as of March 1, 2022, participation in the secondary market for ruble or non-ruble denominated bonds issued after March 1, 2022 by the Central Bank of the Russian Federation, the National Wealth Fund of the Russian Federation, or the Ministry of Finance of the Russian Federation.

Additionally, more sanctions have been placed on Russia including the Office of Foreign Assets Control adding Russian & Belarusian individuals, entities, vessels, and financial institution to the OFAC SDN and NS-MBS lists, Russia being removed from SWIFT, and the U.S. barring the import of Russian crude oil.



Russian Sanctions & Evasion (continued)



FinCEN released an alert on March 7, 2022 addressing potential Russian & Belarusian sanctions evasion attempts and how to identify them. The evasion attempts are grouped within the following categories:

- Attempts via the U.S. Financial System
- Evasion using crypto & virtual currency (CVC)
- Ransomware attacks & other cybercrime

This alert also details how to address Russian sanctions within:

- SAR Reporting – Addition of key term “FIN-2022-RUSSIASANCTIONS” within SAR field 2
- Information Sharing – stressing upon 314(b)
- Customer Due Diligence – Increased importance on senior political figures, private banking accounts and correspondent accounts



Sanctions Red Flags



FinCEN released these 13 red flags for identifying sanctions evasion:

- 1 Use of corporate vehicles (i.e. legal entities, such as shell companies, and legal arrangements) to obscure (i) ownership, (ii) source of funds, or (iii) countries involved, particularly sanctioned jurisdictions.
- 2 Use of shell companies to conduct international wire transfers, often involving financial institutions in jurisdictions distinct from company registration.
- 3 Use of third parties to shield the identity of sanctioned persons and/or PEPs seeking to hide the origin or ownership of funds, for example, to hide the purchase or sale of real estate.¹⁷
- 4 Accounts in jurisdictions or with financial institutions that are experiencing a sudden rise in value being transferred to their respective areas or institutions, without a clear economic or business rationale.
- 5 Jurisdictions previously associated with Russian financial flows that are identified as having a notable recent increase in new company formations.
- 6 Newly established accounts that attempt to send or receive funds from a sanctioned institution or an institution removed from the Society for Worldwide Interbank Financial Telecommunication (SWIFT).
- 7 Non-routine foreign exchange transactions that may indirectly involve sanctioned Russian financial institutions, including transactions that are inconsistent with activity over the prior 12 months. For example, the Central Bank of the Russian Federation may seek to use import or export companies to engage in foreign exchange transactions on its behalf and to obfuscate its involvement.
- 8 A customer's transactions are initiated from or sent to the following types of Internet Protocol (IP) addresses: non-trusted sources; locations in Russia, Belarus, FATF-identified jurisdictions with AML/CFT/CP deficiencies,¹⁸ and comprehensively sanctioned jurisdictions; or IP addresses previously flagged as suspicious.
- 9 A customer's transactions are connected to CVC addresses listed on OFAC's Specially Designated Nationals and Blocked Persons List.
- 10 A customer uses a CVC exchanger or foreign-located MSB in a high-risk jurisdiction with AML/CFT/CP deficiencies, particularly for CVC entities and activities, including inadequate “know-your-customer” or customer due diligence measures.
- 11 A customer receives CVC from an external wallet, and immediately initiates multiple, rapid trades among multiple CVCs with no apparent related purpose, followed by a transaction off the platform. This may be indicative of attempts to break the chain of custody on the respective blockchains or further obfuscate the transaction.
- 12 A customer initiates a transfer of funds involving a CVC mixing service.
- 13 A customer has either direct or indirect receiving transaction exposure identified by blockchain tracing software as related to ransomware.

Common Trend - PHISHING



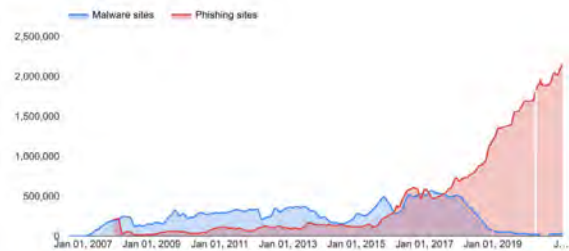
A common trend throughout each section was the involvement in phishing activity.

Criminals will use any current event as a creative method for phishing. The chart on the right shows the explosion of growth since the pandemic began.

How do we combat?

Training is the most important tool in preventing phishing!

100% of phishing attacks can be prevented with proper training on how to identify these attacks.



QUESTIONS
AND ANSWERS



3:40 – 4:55 p.m.

Ethics Update

**Charles Selcer, CPA, CGMA, MBA, Shareholder, Schechter Dokken
Kanter CPAs**

WICPA

FINANCIAL INSTITUTIONS CONFERENCE

CHARLES SELCER, CPA CGMA

MAY 10, 2022



DISCLAIMER

- The views and personal opinions of The Chucker are not in any way the positions or opinions of the Minnesota State Board of Accountancy.



AICPA CODE

- SECTION

- 0. Preface

- 1. Member in Public Practice

- 2. Member in Business

- 3. Others



0 SECTION

- 0.400 Definitions

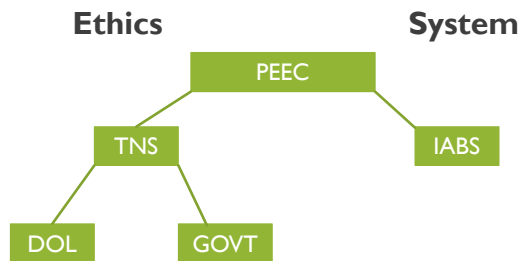
- 0.500 Nonauthoritative Guidance

- 0.600 New Revised & Pending

- 0.700 Deleted



AICPA



JEEP: TYPE 1 OR TYPE 2 STATE

- Iowa – Non-Jeep
- Wisconsin – Type 2
- Minnesota – Type 1

J OF A

- The Journal of Accountancy is no longer mailed to AICPA members as of January 2022
- Behavioral ethics standards are still effective when published in the J of A



POLLING QUESTION

- In Q4 of 2021, Wisconsin's average pass rate on the CPA Exam was
 - A) 61.05%
 - B) 54.72%
 - C) 57.54%
- This was better or worse than Minnesota



UNPAID FEES

- Old Rule

When the current report is to be issued unpaid exist from the attest client for any professional service provided more than 1 year prior to date of current report

- Tantamount to a loan to your loan



UNPAID FEES

- The effect

\$1 due from year client impairs independence



NEW RULE

- Unpaid fees are both significant to the member and relate to professional services more than 1 year prior to the issue date



NEW RULE

Supporters

- E & Y, KPMG, CLA, PWC
- Grant Thornton, Deloitte, Carr Riggs, TXCPA, INCPA

AGAINST

- NASBA, RSM, NYSCA



POLLING QUESTION

- In an example as to why Sconnies score well on the CPA Exam, a question was
If the ratio of hops to grain in a wort is 4:1 how much hops does it take to make 11
Firkins of beer?



THE CHUCKER

- John Mc Enroe answer to old rule
- We are going away from standards to principles
- We triumph substance over form




ANOTHER PEEC PET PROJECT

- Assisting clients with implementing accounting standards



ACCOUNTING STANDARDS IMPLEMENTATION

- New big change standards recently
 - Leases
 - Revenue Recognition
- Challenge in this process 
 - Does client have someone with SKE?



IMPLEMENTATION ASSISTANCE

- Yields self review and management participation threats
- Interpretation lays out
 1. Can dos
 2. Verbotins



VERBOTIN

Means no safeguards could reduce threats to an acceptable level



OUTSIDE CPA CAN NOT

- Lead an implementation team at the client
- Make decisions on how to implement
- Set policy or procedures relating to the standard
- Design new controls or redesign controls over financial reporting
- Design or redesign FIS



POLLING QUESTION

- The fee to take the CPA for 2022 is \$162.52 per section
It comprises
 - A) AICPA Fee \$100 NASBA Fee \$40 Prometric Fee \$12.52
 - B) AICPA Fee \$100 NASBA Fee \$30 Prometric Fee \$22.52
 - C) AICPA Fee \$100 NASBA Fee \$25 Prometric Fee \$27.52



IMPLEMENTATION CAN DOS

- Develop & provide training to client on the standard
- Research, provide advice, make recommendations
- Assist management in drafting strategies
- Propose standard AJE's (templates)



IMPLEMENTATION CAN DOS

- Recommend ideas relating to application of the standard
- Recommend changes or adjustments to information systems as a result of the standard



CAN DOS

Basic Concept → Client Approval



CPA'S AS BANK DIRECTORS

- Cite 1.10.020

A CPA Bank director may have an adverse interest threat if his/her clients are bank borrowers




POLLING QUESTION

- The Journal of Accounting is no longer sent to AICPA member vice mail. To keep current on new ethics railing go to
 - A) ethics.cpa.staykosher.com
 - B) journalofbeancounters.org
 - C) journalofaccountancy.com



INDEMNIFICATION CLAUSES

- Certain clauses are ok per AICPA code, some are not
- Not ok for covered member to indemnify his/her client for their acts
- Basic Concept  It may instill a belief in the auditor's mind that they don't need to do GAAS; we'll be indemnified



INDEMNIFICATION CLAUSES ARE VERBOTEN PER BANK REGULATORS

- It is an act discreditable for a CPA to put such a clause in their bank client engagement letters for a CPA on the receiving end to sign



DISCLOSING BANK CUSTOMER NAMES 2.400.070

- You are a CPA working at the Wounded Badger Bank & Trust, you tell someone the name of that is a bank customer

Is this unethical under AICPA code?

No, if the disclosure doesn't include confidential client information. (not known to the public)



POLLING QUESTION

- True or False?

The AICPA moved its headquarters from New York to Raleigh/Durham because Barry Meloncon was a Tar Heel fan



LICENSING

- Concept is under fire in some quarters

- ARPL study:

1. There is empirical evidence that licensing for female and minority workers helps level the playing field
2. Wages are 10-15% lower for unlicensed workers compared with licensed workers with similar levels of education & training
3. Hourly workers get 6.5% more from having a license

ARPL = Alliance for Responsible Professional Licensing





PARTING THOUGHTS

“If you take the ethical high road, you never have to worry about a traffic jam”

Allan Simpson