Crowe

Smart decisions. Lasting value.℠

The Future is Now

Bitcoin, Crypto, Fintech and Tax Implications

Jennifer Burke & Cody Lewis

May 2022

Bitcoin is a techno tour de force.
- Bill Gates

Bitcoin will do to banks what email did to the postal industry.
- Rick Falkvinge

At the end of the day, customer centric fintech solutions are going to win.
– Giles Sutherland

People need banking, not banks.
- Ranjit Sarai

[Virtual Currencies] may hold long-term promise, particularly if the innovations promote a faster, more secure and more efficient payment system.
- Ben Bernanke (Chairman of the Federal Reserve)

A strategy is necessary because the future is unpredictable.
- Robert Waterman

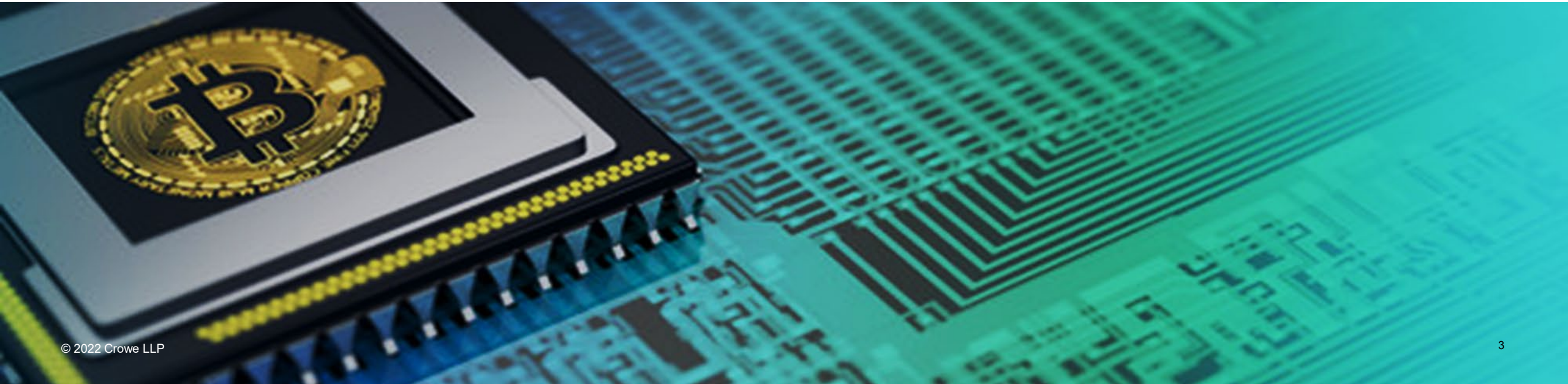
The biggest risk is not taking any risk. in a world that's changing really quickly, the only strategy that is guaranteed to fail is not taking risks.
- Mark Zuckerberg

Hope is not a strategy.
- Vince Lombardi

The best defense is a good offense.
- George Washington

What is Cryptocurrency? (aka Virtual Currency)

- Cryptocurrency is a form of payment that can be exchanged online for goods and services
- Bitcoin is one type of cryptocurrency
- Many companies have issued their own currencies, called tokens, that can be traded specifically for the good or service that the company provides
- Cryptocurrencies work using a technology called blockchain, a decentralized technology spread across many computers that manages and records transactions



Cryptocurrency statistics

- More than 4,000 cryptocurrencies
- Between 2012 and March 2021, Bitcoin has gained 254,445%
- Total cryptocurrency market cap is $1.77 trillion, equivalent to the 8th largest economy globally
- Bitcoin’s total market capitalization is over $600 billion
- Nearly 14,000 Bitcoin ATMs globally
- 101 million identity-verified crypto users in 2020
- Average daily cryptocurrency trade volume is $109 billion per day
- $281m of crypto was stolen in 2020, but ~80% has since been claimed and recovered
- 67% of Millennials look to Bitcoin as a safe haven asset as compared to Gold
- Etsy, Overstock.com, Yum Brands, Whole Foods Market, PayPal, Starbucks, USAA, Home Depot, Microsoft, Tesla and AT&T are NYSE companies that accept Bitcoin payments

Why are cryptocurrencies so popular?

- Supporters see cryptocurrencies such as Bitcoin as currency of the future
- Removes central banks from managing the money supply
- Blockchain technology is a decentralized processing and recording system and *can be* more secure than traditional payment systems
- Speculators like cryptocurrencies because they are going up in value and have no interest in the currencies' long-term acceptance as a way to move money

POPU

What are potential risks of cryptocurrency?

- May go up in value, but some see them as mere speculations because they generate no cash flow
- Currency needs stability but cryptocurrency is not stable today
- Does not need an intermediary and are not tethered to capacity of a centralized government, bank or agency
- Price volatility may result in less spending and circulation, making less viable as a currency
- Guidance/regulations is limited, potentially opening banks to regulatory criticism

> Warren Buffett compared Bitcoin to paper checks:
> It's a very effective way of transmitting money and you can do it anonymously and all that. A check is a way of transmitting money too. Are checks worth a whole lot of money? Just because they can transmit money?

How might cryptocurrencies impact the banking industry?

- OCC issued several interpretive letters detailing how traditional financial institutions can enter into transactions (or develop services) involving digital currencies
- National banks and federal savings associations can now use public blockchains and stablecoins to perform payment activities, providing ability to process payments much quicker and without the need of a third-party agency
- Essentially, the clarifying letter puts blockchain networks in the same category as SWIFT, ACH, and FedWire
- Adoption could streamline, enhance, and upgrade financial services

How can banks get involved in the cryptocurrency industry?

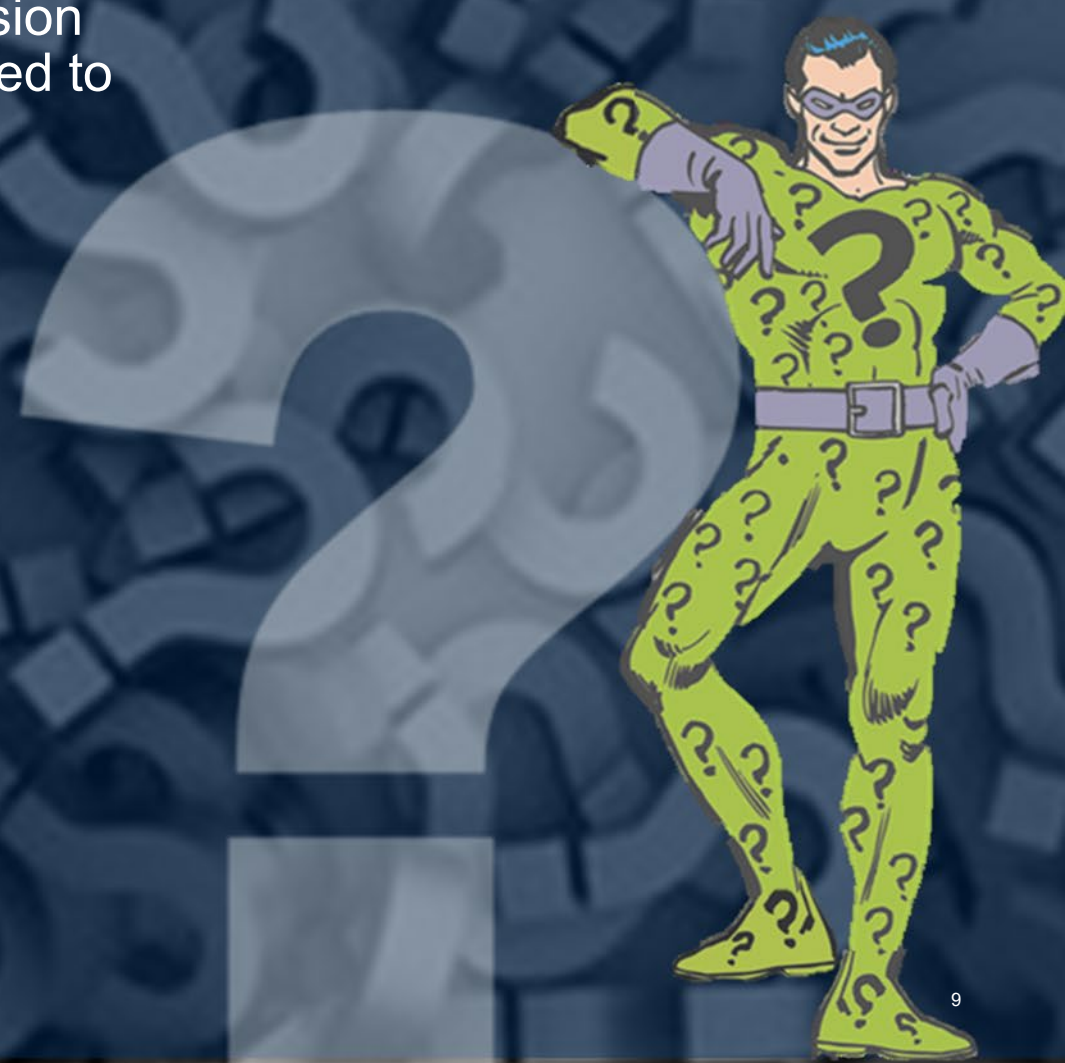
- Offer **crypto custody services** for customers, including holding unique cryptographic keys associated with accessing private wallets
- Provide **onboarding, purchasing and expert assistance** to assist new, less experienced individual investors by developing tools to facilitate the adoption of crypto
- Offer **interest-bearing crypto accounts** where customers could invest crypto through other financial tools
- Help **mitigate security concerns** of cryptocurrency holders regarding theft or hack of digital currencies by bringing cryptocurrency under bank supervision
- Utilize public blockchains to **speed up payment processes**. Blockchain technology provides a faster and less expensive alternative to clearing houses
- Lend **cash collateralized by virtual currency**.

Examples:

- JP Morgan has taken on **two cryptocurrency exchanges** (Coinbase and Gemini) as banking customers
- Fidelity Digital Assets is **creating a crypto fund**
- PayPal is now allowing **cryptocurrency transactions** on their network
- **NYDIG now partners with core processor FIS** to allow banks to offer customers the ability to buy, sell and hold bitcoin.
- Signature Bank and Silvergate Bank currently offer **cash loans collateralized by bitcoin.**

Complications for banks transacting in virtual currency

- Risk weighting – BASEL Committee on Banking Supervision proposes risk weighting of Bitcoin and other tokens not tied to traditional assets at 1,250%.
- Accounting considerations – is the virtual currency an indefinite-lived intangible?
  See the **AICPA Practice Aid – Accounting for and auditing of digital assets**
- Price volatility
- Risk management – BSA / AML / Others
- Purchasing issues related to price movement
- Stablecoins – lack of transparency
- Tax issues –
  - Information reporting – Which 1099 do we issue?
  - Income tax - transacting in property
  - State sourcing



What is Fintech (aka Financial Technology)?

- Financial technology (Fintech) refers to the integration of technology into offerings by financial services companies in order to improve their use and delivery to consumers
- Relates mainly to small start-up companies which develop innovative technological solutions in online and mobile payments, big data, alternative finance and financial management
- Startups disrupt incumbents in the finance Industry by expanding financial inclusion and using technology to cut down on operational costs
- Includes different sectors and industries such as education, retail banking, fundraising and nonprofit, and investment management
- Now includes the development and use of crypto-currencies

Fintech statistics

- Over **10,000** fintech startups in the United States
- **88%** of legacy banking companies fear losing profits to fintech firms
- **82%** of traditional financial companies plan to increase collaboration with fintechs in the next 3-5 years
- **60%** of financial institutions view fintech firms as potential partners
- Fintech firms are used by **50%** of all banking customers
- **77%** of people make payments using their mobile devices
- **91%** of Gen Xers understand the perks of mobile banking
- Global fintech market is estimated to be over **$300 billion by 2023**
- In 2021, Apple Pay, Google Pay, and Samsung Pay are projected to own **56%** of the combined market share of mobile payments

Why are fintechs so popular?

- Faster transactions/decisions
- 24/7 access
- Fully-digital solutions
- Very targeted products for gaps in the marketplace
- Focus on mobile functionality, big data, agility, and convenience
- Ability to conduct business, transfer funds and buy products with just one button click
- Enhanced efficiency and convenience
- More flexibility
- Expand access to underserved populations

ULAR

What are potential risks of fintechs?

- Errors related to focus on speed to decisions
- Lack of regulation and commonly applied standards
- Potential fintech bubble
- Consumer disclosure and transparency violations
- Digital fraud (cybersecurity)
- Platform/technology unreliability or vulnerability
- Lack of customer satisfaction due to limited/no human interaction to address problems
- Algorithmic decision-making leading to potentially discriminatory or biased outcomes

> Jamie Dimon, JPMorgan Chase chairman and CEO, listed fintech as one of the “enormous competitive threats” to banks in his annual shareholder letter. He also pointed out the lack of regulatory requirements for fintechs.

How might fintechs impact the banking industry?

- Improved and expanded customer service
- Improved mobile banking solutions
- More narrowly defined, targeted solutions and offerings
- Improved use of customer data for decision-making
- More partnering and collaborating with fintechs
- Example:
  - Robo-advisors—digital platforms that provide automated, algorithm-informed investment suggestions and financial planning advice, with little to no human oversight.

Common accounting and tax trends in fintech

- Revenue recognition complexities (GAAP)
  - Gross vs. Net
  - Non-interest bearing vs. interest bearing
- No deposit base for funding
- Nonbanks buying the smallest bank they can find for the charter
- Nonbank tax treatment – potential capital asset treatment
- Section 475 mark-to-market rules
- Loss corporations and section 382
- Significant multi-state reporting obligations
- International considerations

In conclusion…

Virtual currencies have promising technology and use cases, but significant complexities abound. You should consult your GAAP, tax and risk professional advisors when you pursue further investment.

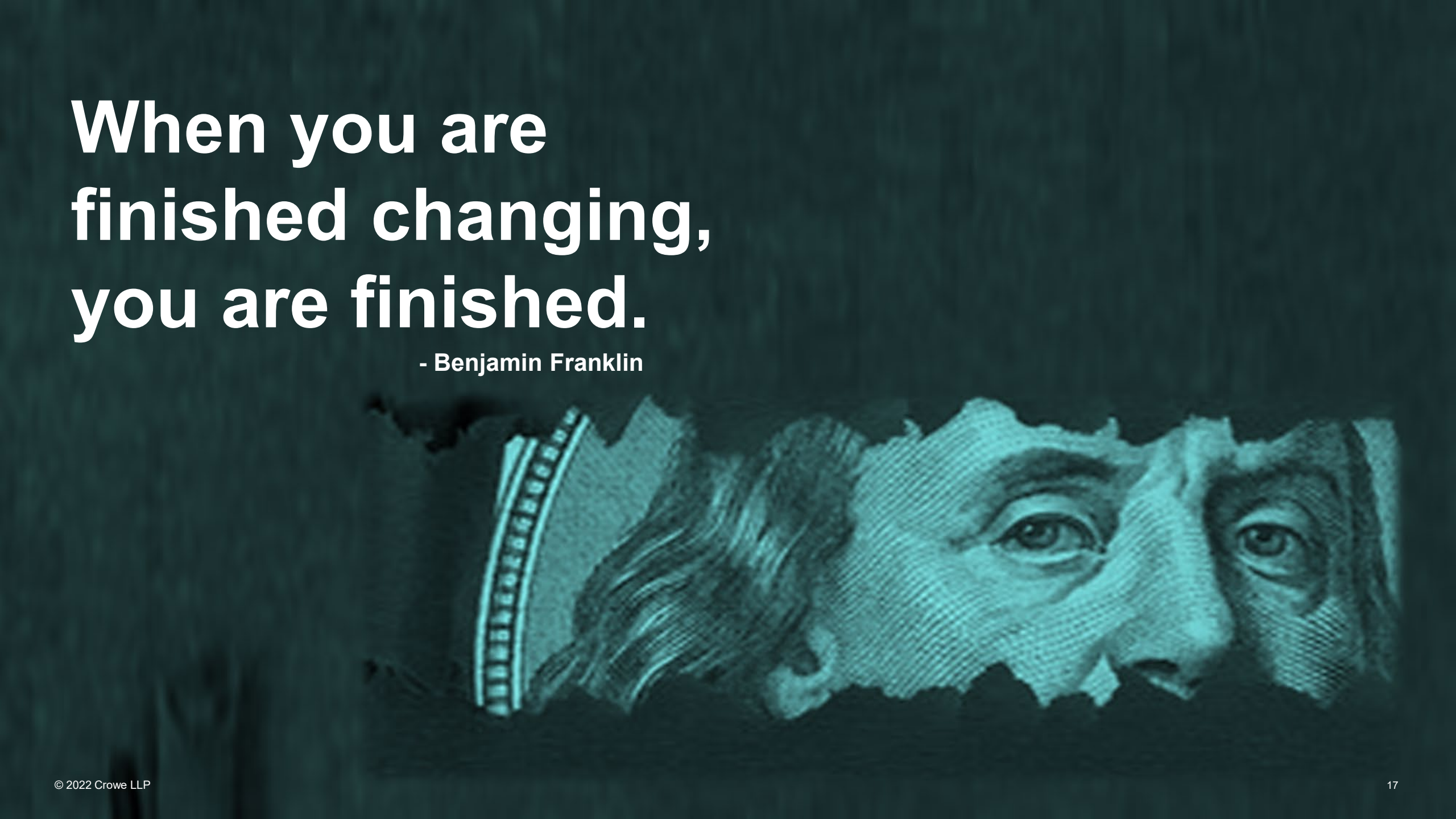
Fintech companies are competing directly with banks in many instances, but there are many more opportunities for partnerships and fintech companies are consistently seeking such partnerships for services they cannot offer their customer base.

These two disruptive forces can change how community banking is done in the present and future.

Be open to changing customer needs and expectations as you examine your business strategy.

When you are finished changing, you are finished.

- Benjamin Franklin



Thank you!

Crowe

Smart decisions. Lasting value.℠

The State of Ransomware: 2022

May 2022

Myra Rowell
Senior Manager

Education, Certifications & Professional Affiliations

Masters of Business Administration
Montreat College | Montreat, NC

Bachelor of Science, Management
Montreat College | Montreat, NC

Six Sigma Lean, DFSS

PMP 2003-2016

Profile

Ms. Rowell is a Senior Manager for Crowe's FS IA Technology Consulting Practice. Ms. Rowell has an extensive 20-year career in cyber security protection, objectives, and programs including external risk and engagement, third party, business risk and controls, and change management. Managed existing and emerging risk, risk tolerance strategies for the business with sensitivity while meeting objectives.

Professional & Industry Experience

- Extensive experience with large financial institutions, developing business risk strategies, cross sector engagements, managed and quantified new and unforeseen partner risk
- Third party partner banks, financial market utility (FMU), clearing house and settlements risk, managed unstructured environment by developing strategic direction for non-contractual partner risk, information security risk tolerance, executed and enhanced control governance and compliance, managed emerging and existing information security business controls and risk objectives
- Managed and developed technical strategy using Offshore Intelligence (OSINT), developed and translated information security threat exercise results to business metrics
- Merger and acquisition combined company risk tolerances and cyber security controls including laws, rules, regulations across 42 countries

Client Focus

- Financial Services
- Cyber Security
- Third Party Risk
- Governance, Risk, and Compliance (GRC)
- Privacy
- Mergers and Acquisition
- Business Information Security Risk
- Trade Organizations

Topics

01 What is Ransomeware?

02 Are you Ready?

03 How do you respond?

04 Do you recover?

1. What is Ransomware?

About Ransomware

- Ransomware is the fastest growing malware threat, targeting users of all types - - from the home user to the corporate network.
- Ransomware is designed to encrypt files on the attacked network. Malicious actors then demand ransom in exchange for the key to decrypt the files.
- Organizations are faced with a decision to restore from backups, rebuild without access to the encrypted data, or pay the ransom and hope to recover the data with the encryption key.

Polling Question

1

What is the % increase in Ransomware attacks that have occurred over Year over Year from 2020 – 2021?

- Less than 250%
- 250 – 500%
- 500 – 750%
- Greater than 750%

Polling Question

2

What is the average cost of remediating a ransomware attack in 2021?

- $250,000 – $500,000
- $500,000 - $1,000,000
- $1,000,000 - $1,500,000
- Greater than $1,500,000

How Does it Work?

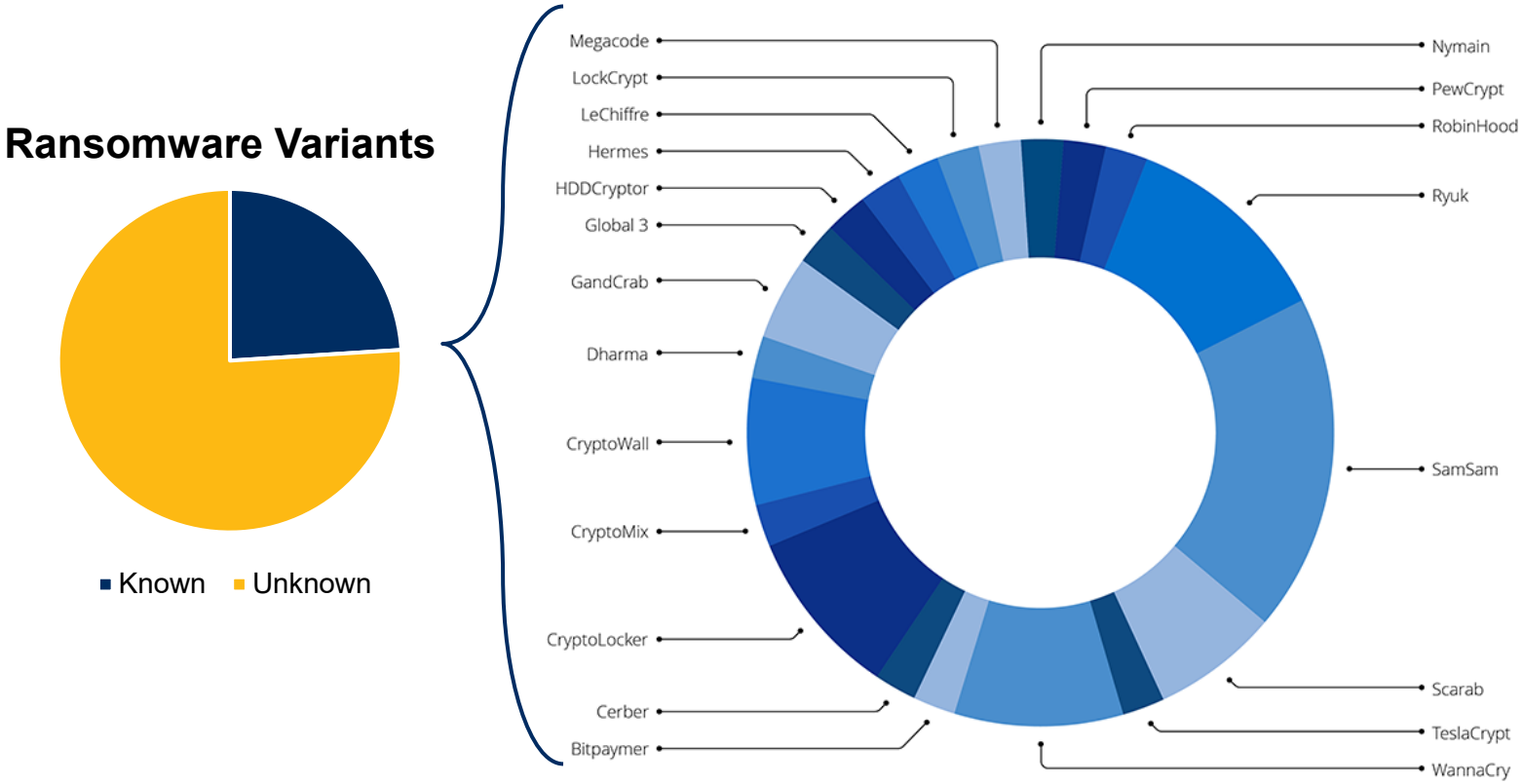
- Ransomware needs an entry point in order to begin the attack.
- Ransomware is most frequently distributed using phishing campaigns, business email compromise, or clicking malicious links.

- Once inside the environment, the ransomware executed on the infected system and targets accessible files which can include network-hosted databases and file shares.
- Once ransomware executes, the malware locks systems and files from being accessible and usable.
- Ransomware can exploit security weaknesses to spread to other devices and broaden the impact.

- Once ransomware has executed, a demand is made of the impacted organization, typically with a quick turnaround time, to pay the ransom in exchange for decryption keys.
- If the data is unavailable via other mechanisms (i.e., backups), the affected user has limited response options.

Ransomware Strains

The chart shows **76%** of ransomware variants used against organizations in the last seven years were unknown while the right shows the most common identified variants seen in breaches, such as: SamSam, WannaCry, Ryuk, CryptoLocker, RobinHood, etc.



https://go.recordedfuture.com/hubfs/reports/cta-2019-0510.pdf

Case Study

Kronos, a workforce management platform, was affected by a ransomware attack on December 11, 2021.

Thousands of employers and approximately **8 million employees** relied on Kronos for online management of work hours, paychecks, tax forms, and more.

Kronos clients, many of whom are healthcare organizations, were forced to revert to manual, paper-based methods of scheduling personnel, tracking time, and issuing paychecks. This impact came as the COVID-19 Omicron variant was heightening administrative scheduling requirements for hospital staff.

Workers at affected companies reported lost and/or missing paychecks.

Restoration of core services took **over a month** and restoration of secondary services continues as of March 2022.

Polling Question

3

How significant do you believe the ransomware risk is to your organization?

- **Highly significant** – we are very worried about ransomware
- **Somewhat significant** – we are worried about ransomware, but we have greater risks to consider
- **Not significant** – we are not very worried about ransomware

Polling Question

4

Do you feel confident in your organization's ability to respond to a ransomware attack?

- Not confident
- Somewhat confident
- Confident
- Very confident

2. Are You Ready?

Ransomware Preparedness

Defense in Depth

- Business Continuity and Disaster Recovery
- Threat and Vulnerability Management
- Employee Awareness and Training
- Continuous Monitoring
- Third Party Risk Management
- Cyber Incident Response
- Cybersecurity Governance and Strategy

Considerations for Audit

- Third line is an active component in improving cybersecurity posture
- Regulatory compliance *with* industry best practices
- Stay connected with cybersecurity trends
- Understand the risk: who, what, why

Risk Based Audit Approach

1

What are you trying to protect?

How important is it?

How attractive are you?

2

Who threatens what you are trying to protect?

How can they threaten you?

What is your risk appetite?

3

What are your vulnerabilities?

What are the risks that the vulnerabilities introduce?

What is changing in your environment?

4

How are you protecting yourself against those risks?

What are the consequences of failing to implement appropriate controls?

3. How Do You Respond?

Paying the Ransom?

Government Recommendations

- The US Government strongly encourages victims NOT to pay the ransom but acknowledges the risk-based business decision.
- The recommended approach in ransomware response includes contacting the FBI for incident response assistance.
- Notify local authorities

Paying the Ransom

- Your institutions legal team should be involved as part of the Incident Response plan / team to help guide decisions.
- Paying could inadvertently encourage this criminal business model.
- Check federal and state laws as paying a ransom may be illegal.

Odds of Success

- Paying the ransom does NOT guarantee the organization will regain access to their data.
- Many organizations who pay ransom are targeted a second time by ransomware or, after initial payment, asked to pay more than the original ransom amount to get the promised decryption key.
- Out of all ransomware victims, **32** percent pay the ransom, but they only get **65** percent of their data back

https://www.cloudwards.net/ransomware-statistics/#Sources

4. How Do You Recover?

Recovery is a long road… if not prepared…

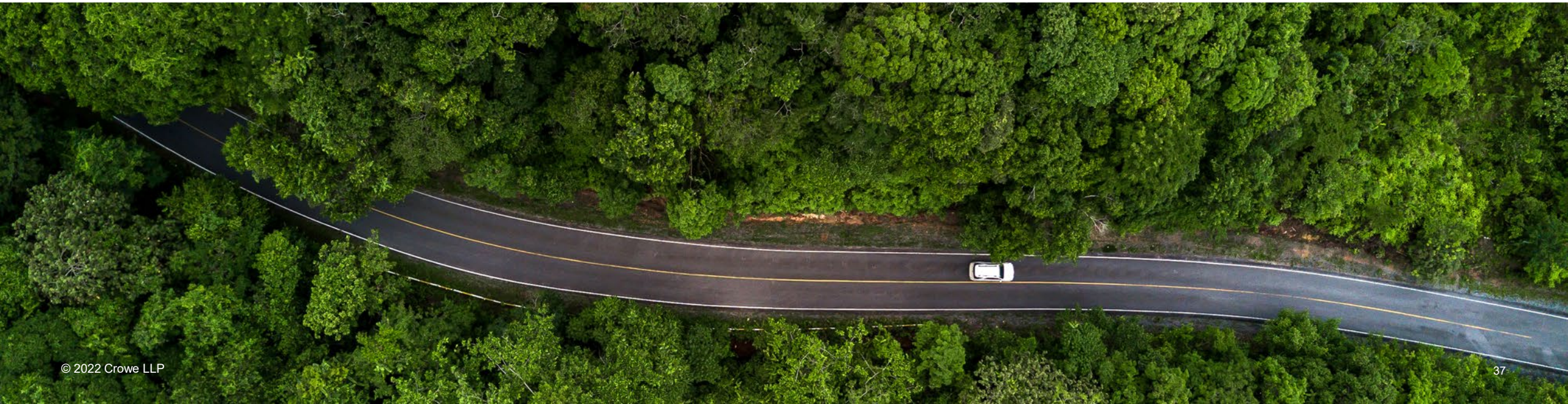
Enact Business Continuity Program

- Business Impact Assessment
- Business Continuity Plans
- Resiliency Requirements
- Backup & Recovery Plans

IT to consider the execution of the Disaster Recovery Program

Initiate Communication Plans

- Internal
  (i.e., employees, contractors)
- External
  (i.e., vendors, law enforcement, regulators)



Post-Recovery

Postmortem Review

- Determine root cause
- Document Lessons Learned
- Implement mitigating controls

Employee Awareness & Security Training

Perform Simulated Ransomware Exercises

Consider an Independent Security Assessment

Strengthen Cybersecurity Governance, Strategy & Controls

Risks Addressed:

- ✓ Fool me twice, shame on me
- ✓ Resolving unknown vulnerabilities with People, Process, and Technology
- ✓ Prevent easily exploitable Vulnerabilities within IT Infrastructure

Thank you!