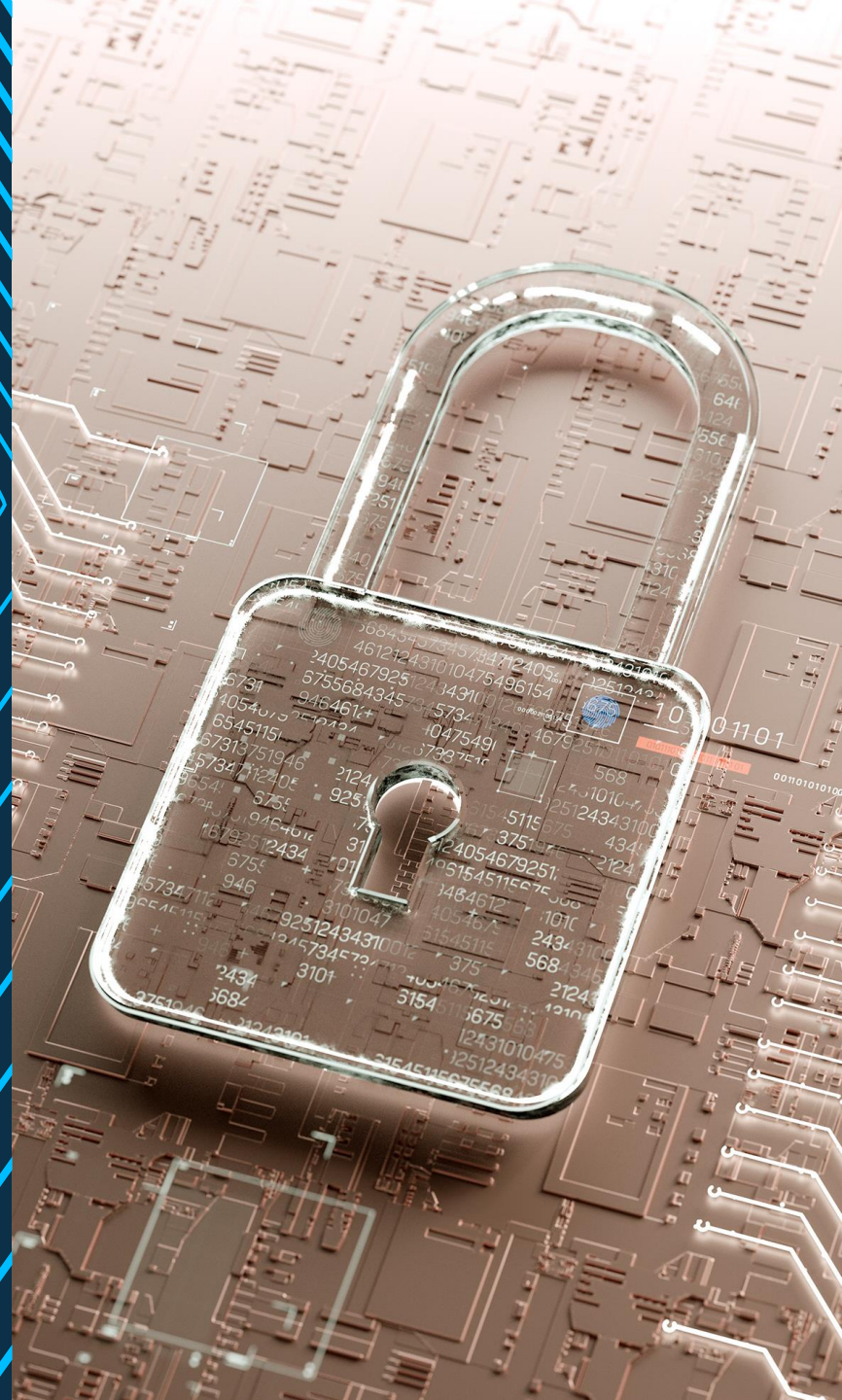
SVB Presents: Cyber Fraud Insights from the FBI

November 2022



SVB - Financial Intelligence Unit

Today's Speakers

Marlene Veum
Head of Cyber Security Operations & Threat Intelligence, SVB

Marlene leads a team of senior security managers, engineers, specialists, and analysts, maintaining corporate-wide cyber security operations to ensure that SVBs digital ecosystem and assets are adequately protected from breaches, threat actor exploitation, and internal threats. Marlene is a Certified Information Systems Security Professional (CISSP) and is completing an MSc in Blockchain and Digital Currency.

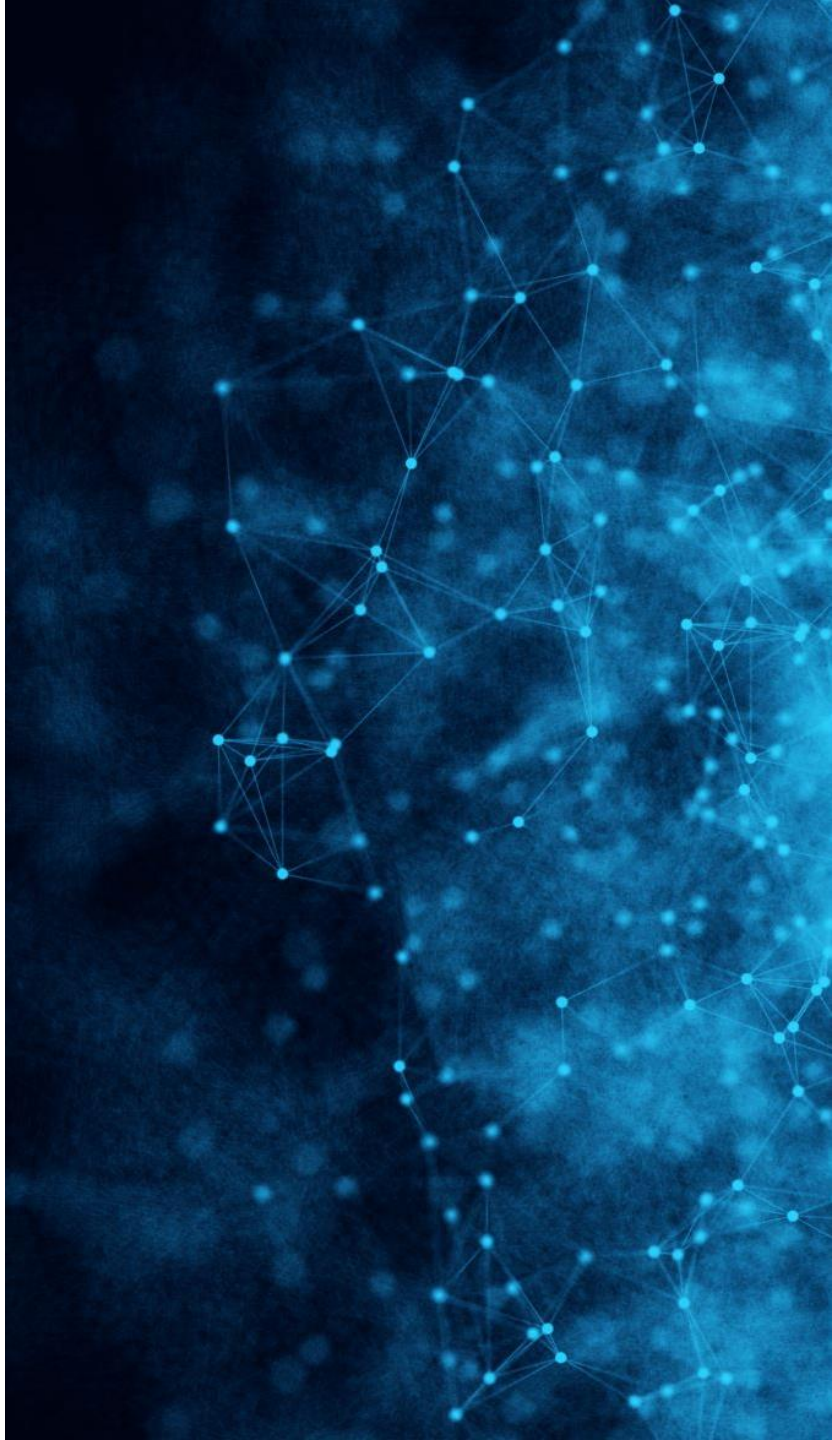
Scott Hellman
Supervisory Special Agent, FBI

Supervisory Special Agent Scott Hellman has been investigating criminal and national security cyber crimes for over 14 years with the FBI. He earned a Bachelor's in Chemistry, a J.D. from the University of Baltimore, and now leads a team of cyber crime investigators in the San Francisco Bay Area.

svb

Agenda

- 2022 Fraud Trends by Industry
- Financial Services Fraud Concerns
- Prevention Tips



svb

svb

Fraud Trends in Banking 2022

Marlene Veum

Head of Cybersecurity Operations, Silicon Valley Bank

2022

Types of Fraud by Industry

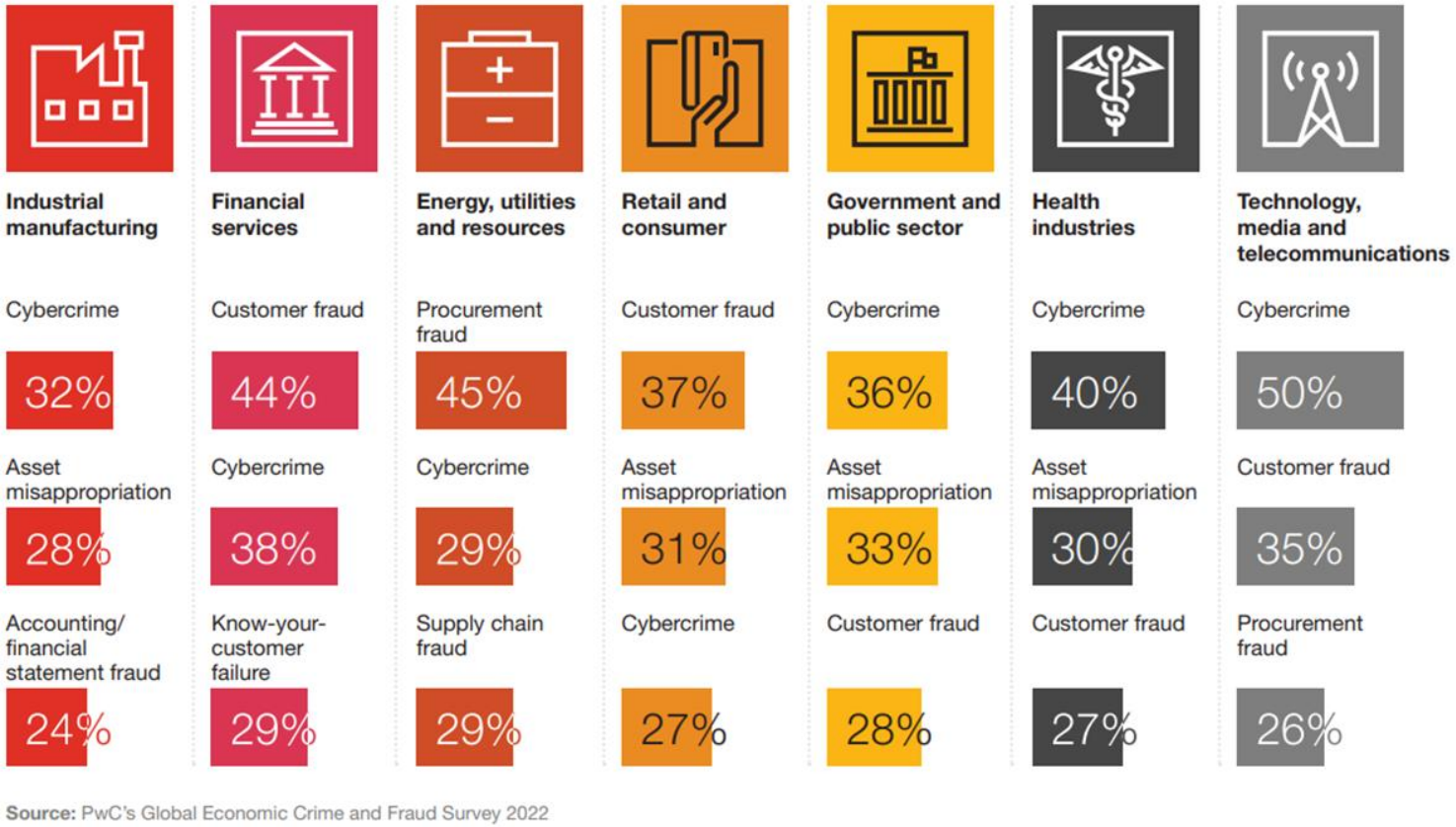
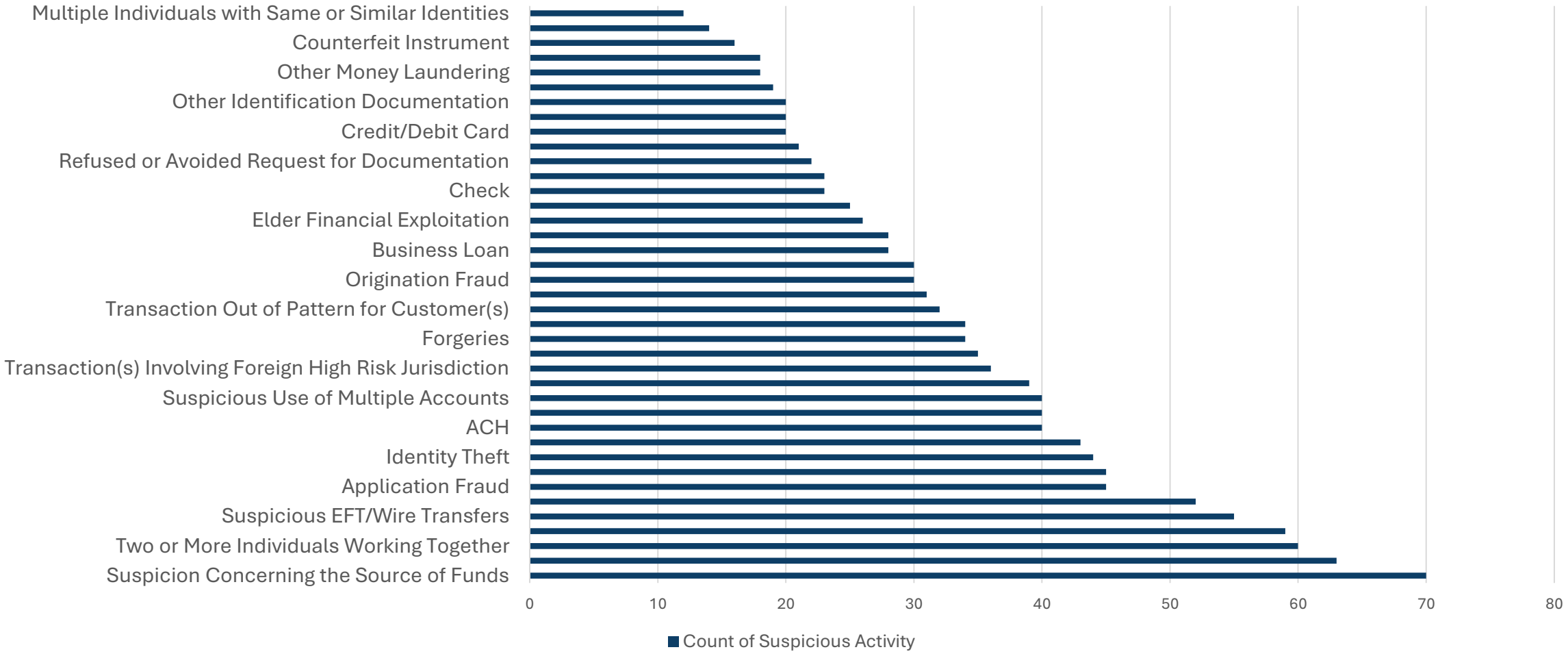


Figure 1: PWC's Global Economic Crime and Fraud Survey Types of Fraud by Industry

YTD 2022 Suspicious Activity Report (SAR) Data



FINANCIAL CRIMES ENFORCEMENT NETWORK (FinCEN)
SUSPICIOUS ACTIVITY REPORT (SAR) FILING TREND DATA
https://www.fincen.gov/reports/sar-stats

svb

Ransomware

Ransomware continues to pose a significant threat to U.S. critical infrastructure sectors, businesses and the public, according to a report released by the Financial Crimes Enforcement Network (FinCEN).

According to the analysis, FinCEN received 1,489 ransomware-related filings worth nearly $1.2 billion in 2021.

This represents a 188% increase compared to the total of $416 million in 2020.

Roughly 75% of incidents reported during the second half, pertain to Russia-related ransomware variants.

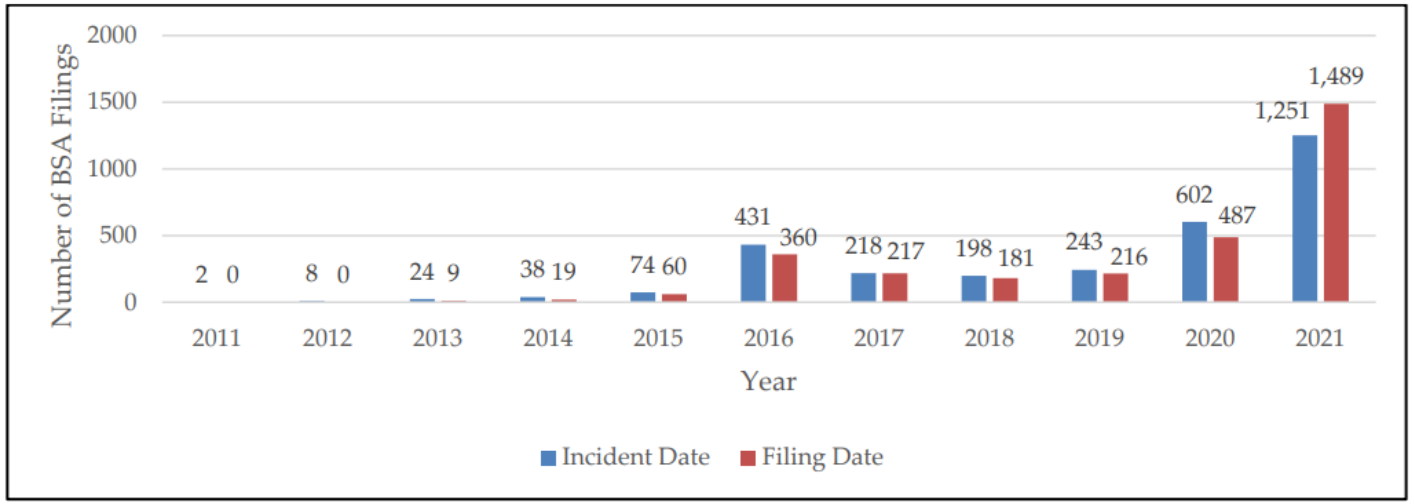


Figure 2: Number of Ransomware-Related BSA Filings by Filing and Incident Dates, 2011 to 2021

svb

When it’s successful, smishing tricks the recipient into taking some action such as visiting a fraudulent site and giving up your credentials or downloading a rogue application that can compromise your phone or steal personal information.

Smishing

Smishing is a form of phishing that targets smartphone users via text or SMS messages.

Quick Response (QR) Code Manipulation

A new type of skimming.

The shift to digital banking and payments is enabling cybercriminals to steal consumers' login and financial information using a fraudulent QR code.

3rd and 4th Party Digital Supply Chain Risk

- Gartner predicts that by 2025, 45% of organizations worldwide will have experienced attacks on their software supply chains, a three-fold increase from 2021.
- Security and risk management leaders must partner with other departments to prioritize digital supply chain risk.
- Vendor risk management monitoring services are expected to grow 14.7% CAGR 2021-2026.
- Continuous monitoring of suppliers is needed to ensure vendors demonstrate security practices and meet compliance requirements for rapidly changing regulations across different regions.

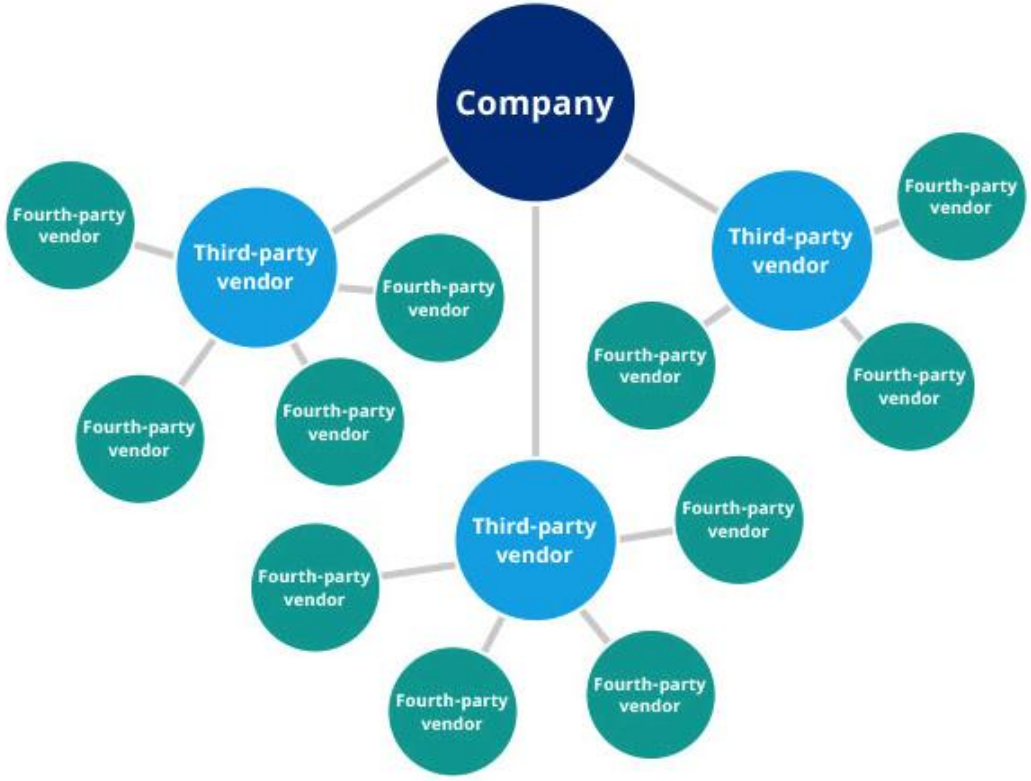


Figure 3: Third and Fourth-Party Risk Ecosystem

Prevention Tips

Develop a Multi-year strategy and “Community of Practice” with Cyber, Fraud, Privacy, Third-Party-Risk, Business, Data HR, Legal, and Outside Agencies.

Prevent and detect fraud with a holistic view of threats (e.g. external, internal, consumer, 3rd & 4th party-supply-chain) across your organization.

Establish a comprehensive incident management response plan and risk framework to include communication, education, training, risk rating, impact analysis, and reporting protocols with external and internal fraud and risk partners.

Tools & Resources

SVB has resources to help you prevent fraud:

- Visit the Fraud Prevention Center on svb.com for best practices and articles on fraud trends
- A BEC Training Video is available to help you educate your employees about business email compromise scams
- Solutions like Fraud Control Services can help you monitor check and ACH transactions to automate fraud detection
- Consider obtaining an insurance policy that includes cybersecurity coverage, such as startup insurance provider Vouch
- If you have additional questions, please don't hesitate to reach out to your Relationship Advisor or Client Support team

svb

Thank you.

Silicon Valley Bank

This content is intended for US audiences only.

This material, including without limitation to the statistical information herein, is provided for informational purposes only. The views expressed in this video are solely those of the author(s) and/or participant(s), and do not necessarily reflect the views of SVB Financial Group, Silicon Valley Bank, SVB Securities or any of its affiliates.

The material is based in part on information from third-party sources that we believe to be reliable but which has not been independently verified by us, and, as such, we do not represent the information is accurate or complete. The information should not be viewed as tax, investment, legal or other advice, nor is it to be relied on in making an investment or other decision. You should obtain relevant and specific professional advice before making any investment decision.

Nothing relating to the material should be construed as a solicitation, offer or recommendation to acquire or dispose of any investment, or to engage in any other transaction.

svb