

RSM

FINANCIAL CRIME AND FRAUD TRENDS

WICPA

May 2022

1

---

---

---

---


---

---

---

Speaker

RSM



**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.

2

---

---

---

---

---

---

---

RSM

ELECTRONIC FUNDS TRANSFER (EFT) FRAUD

3

---

---

---

---

---

---

---

### 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.

---

---

---

---

---

---

---

---

4

### 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.

---

---

---

---

---

---

---

---

5

### 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:

---

---

---

---

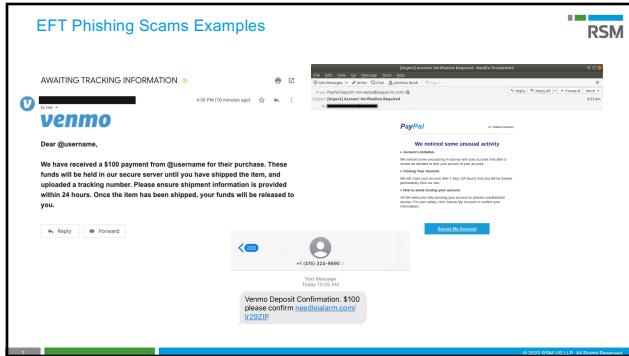
---

---

---

---

6



7

---

---

---

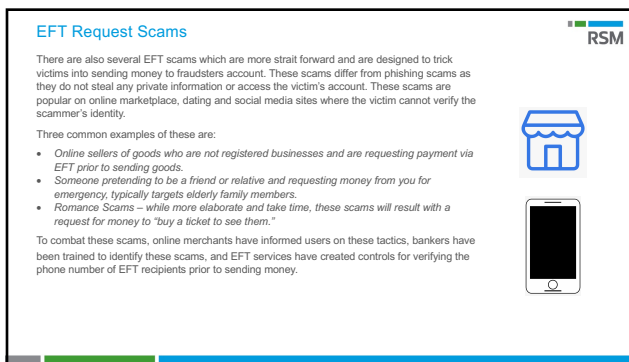
---

---

---

---

---



8

---

---

---

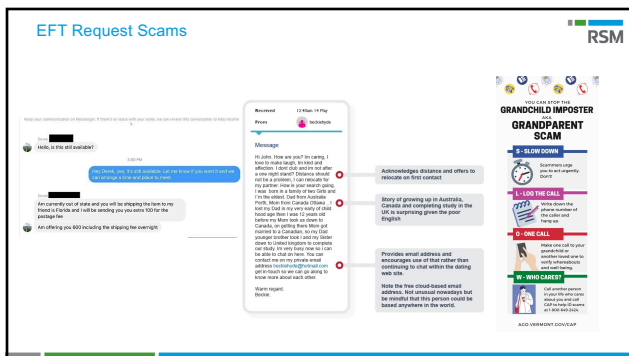
---

---

---

---

---



9

---

---

---

---

---

---

---

---

RSM

COVID-19 & CARES ACT SCAMS AND FRAUD

10

---

---

---

---

---

---

---

---



CARES Act Fraud

RSM

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

11

---

---

---

---

---

---

---


---

Stimulus Payment Fraud

RSM

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.



12

---

---

---

---

---

---

---

---

---

---

---

---

---

---

---

---

---

---

---

---

---

---

---

---

---

---

---

---

---

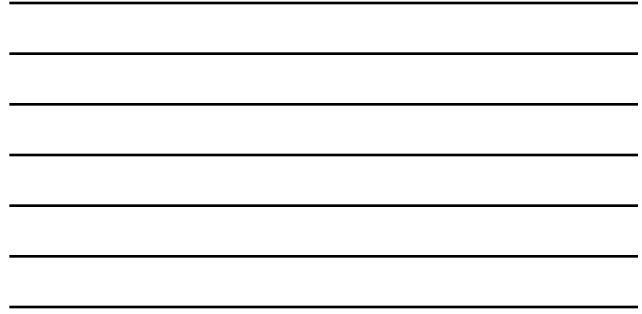
---

---

---

---

---



### Healthcare Benefits Fraud (continued)

### 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-GAO

19

---

---

---

---

---

---

---

---

## DIGITAL ASSETS FRAUD

20

---

---

---

---

---

---

---

---

### 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

21

---

---

---

---

---

---

---

---

### 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.

RSM

22

---

---

---

---

---

---

---

---

### 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.

RSM

23

---

---

---

---

---

---

---

---

### 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 transactions is the best first-line defense as we wait for solid regulations.

RSM

24

---

---

---

---

---

---

---

---

### 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 SSQUID coin which had no true ties to the Netflix show, Squid game, but jumped from one penny to above \$2,600.00 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**

- Account Takeover**
  - Phishing
  - Credential Stuffing
- Mining Fraud**
  - Rentless
  - Crypto Jacking
- Initial Coin Offering Fraud**
  - Bait Schemes
  - Pump and Dump

25

---

---

---

---

---

---

---

---

### 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

---

---

---

---

---

---

---

---

### Eight Popular Crypto Scams

8 TYPES OF CRYPTOCURRENCY FRAUD AND SCAMS

- PHISHING CRIMES**  
Scammers use a variety of tactics to trick victims into revealing sensitive information like usernames, passwords, and private keys. This information can then be used to steal funds from the victim's wallet.
- SCAMMATICAL COIN OFFERINGS**  
Scammers create a fake coin and promote it through social media and online forums. They then use a variety of tactics to lure victims into investing in the coin, including offering high returns and promising to make the coin go viral.
- PUSSY AND SHIT SCHEMES**  
Scammers create a fake coin and promote it through social media and online forums. They then use a variety of tactics to lure victims into investing in the coin, including offering high returns and promising to make the coin go viral.
- MARKET MANIPULATION**  
Scammers use a variety of tactics to manipulate the market, including spoofing, front running, and churning. This involves mass movements of currencies to inflate/deflate values of specific coins to influence trader's decisions.
- PHISH SCHEMES**  
Scammers use a variety of tactics to trick victims into revealing sensitive information like usernames, passwords, and private keys. This information can then be used to steal funds from the victim's wallet.
- TRADITIONAL THEFT**  
Scammers use a variety of tactics to steal funds from victims, including phishing, social engineering, and physical theft. This can involve stealing funds from a victim's wallet or from a bank account.
- BREWER CRIMES**  
Scammers use a variety of tactics to steal funds from victims, including phishing, social engineering, and physical theft. This can involve stealing funds from a victim's wallet or from a bank account.
- UNUSUAL CRYPTO PROTECTIONS**  
Scammers use a variety of tactics to steal funds from victims, including phishing, social engineering, and physical theft. This can involve stealing funds from a victim's wallet or from a bank account.

27

---

---

---

---

---

---

---

---

RSM

RECENT TRENDS & CONCLUSION

28

---

---

---

---

---

---

---

RSM



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.



29

---

---

---

---

---

---

---


RSM

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.



30

---

---

---

---

---

---

---

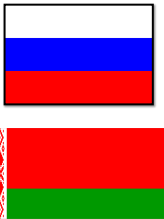
### Russian Sanctions & Evasion (continued)

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



RSM

31

---

---

---

---

---

---

---

---

### Sanctions Red Flags

FinCEN released these 13 red flags for identifying sanctions evasion:

- 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.
- Use of shell companies to conduct international wire transfers, often involving financial institutions in jurisdictions distinct from company registration.
- 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.
- 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.
- Jurisdictions previously associated with Russian financial flows that are identified as having a reliable recent increase in new company formations.
- 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).
- 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.
- 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/CFP deficiencies; and comprehensively sanctioned jurisdictions; or IP addresses previously flagged as suspicious.
- A customer's transactions are connected to CVC addresses listed on OFAC's Specially Designated Nationals and Blocked Persons List.
- A customer uses a CVC exchanger or foreign located MSB in a high-risk jurisdiction with AML/CFT/CFP deficiencies, particularly for CVC entities and activities, including inadequate "know-your-customer" or customer due diligence measures.
- 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 blockchain or further obfuscate the transactions.
- A customer initiates a transfer of funds involving a CVC mixing service.
- A customer has either direct or indirect receiving transaction exposure identified by blockchain tracing software as related to ransomware.

RSM

32

---

---

---

---

---

---

---

---


### 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.



RSM

33

---

---

---

---


---

---

---

---

QUESTIONS  
AND ANSWERS



34

---

---

---

---

---

---

---