Building Success. Together.

The State of Fraud

Virginia Bankers Association

Connect | Protect Experience

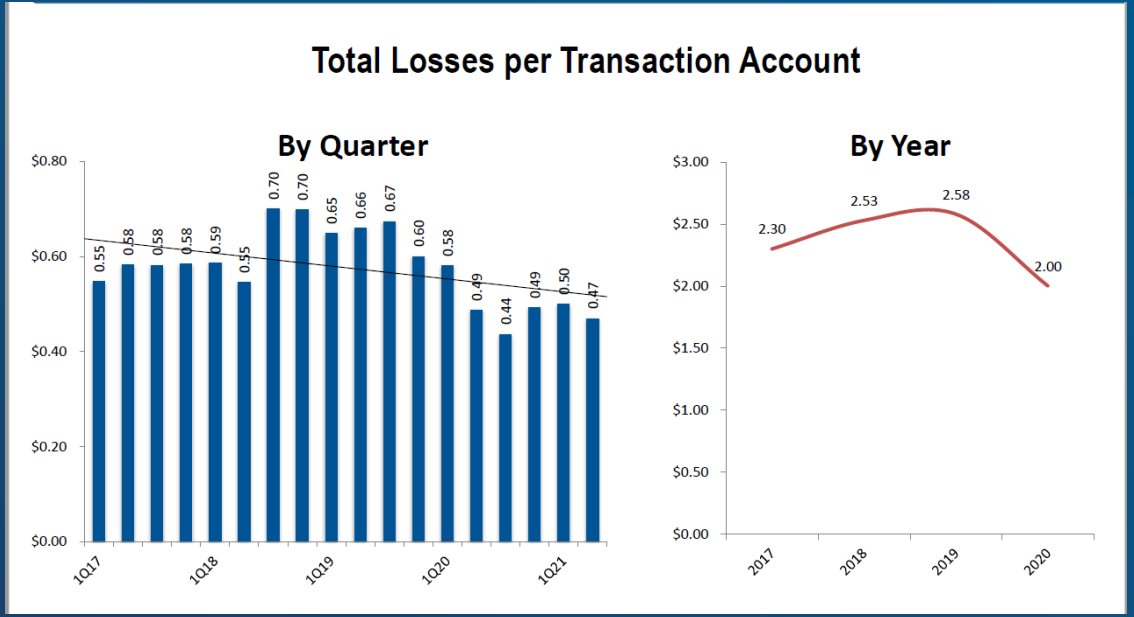
February 28, 2022

Agenda

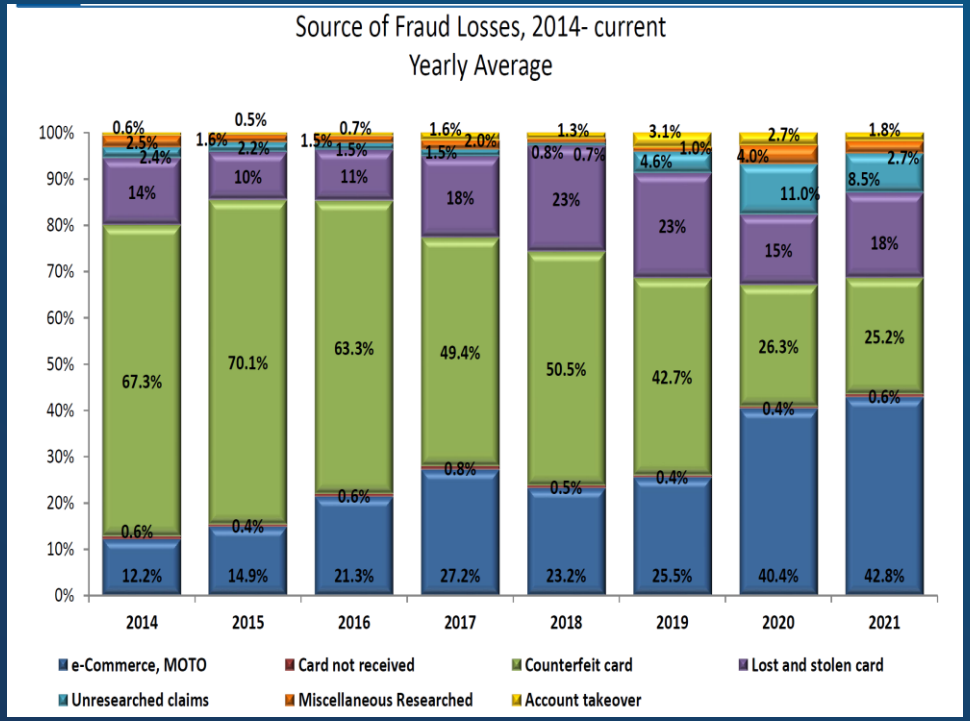
- Defining the Problem
- Building a Strong Defense
- Top Targets / Threats & How to Mitigate
  - State Unemployment Insurance Fraud
  - P2P Trending Fraud – Zelle
  - Email Compromise Fraud (Business Email Compromise / Email Account Compromise)
- Tools & Notes
- Appendix

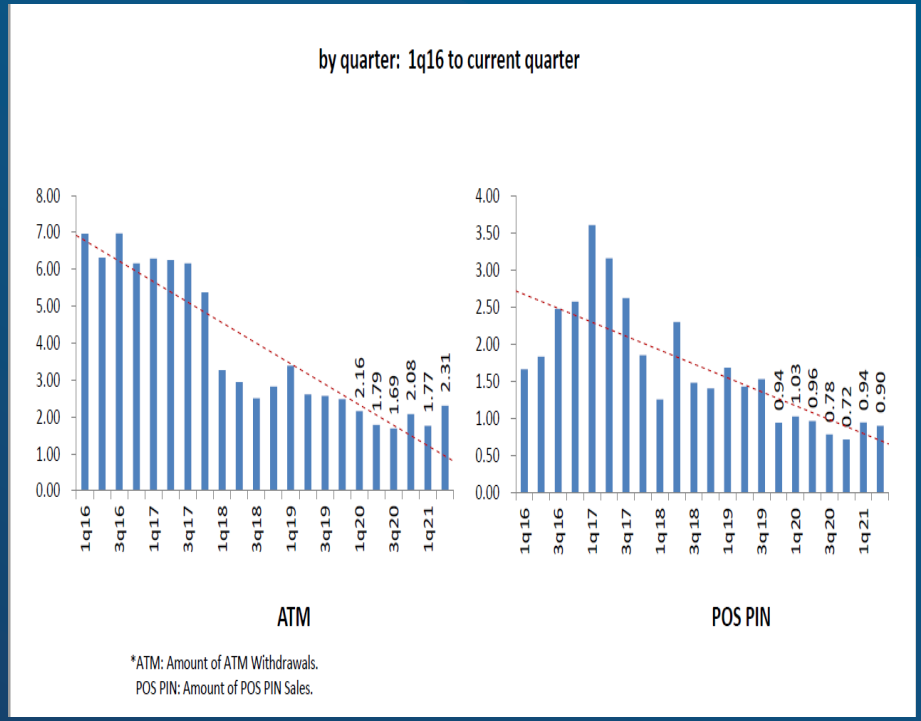
Check Fraud was No Longer King in 2021…But is Making a Comeback

- Check fraud slowly dropped when the pandemic started in Q2 2020.
- It remained low and steady until recently (anecdotally).



Debit Card Fraud remains a good Monetization Tool for Fraudsters…





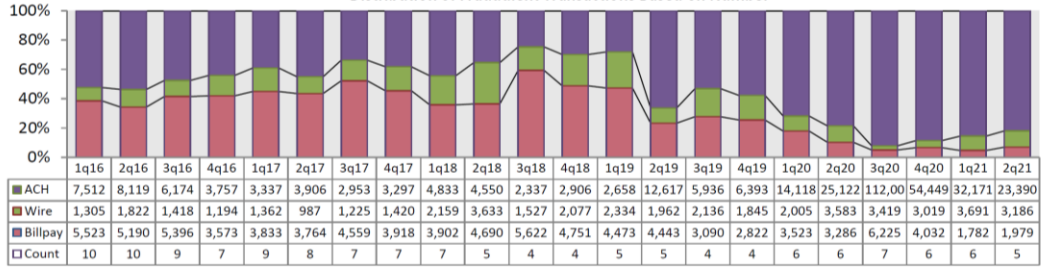
Online Banking Fraud

- ACH has been the leading category in fraudulent transactions based on number of transactions since early 2019.
- ACH fraudulent transactions (based on number) have represented over 60% since 2020.

Overview of Loss Reporting Results

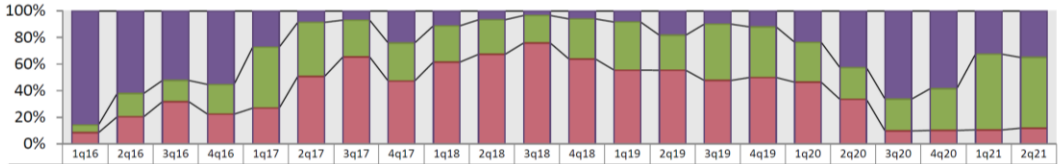
1q16-current

Distribution of Fraudulent Transactions Based on Number

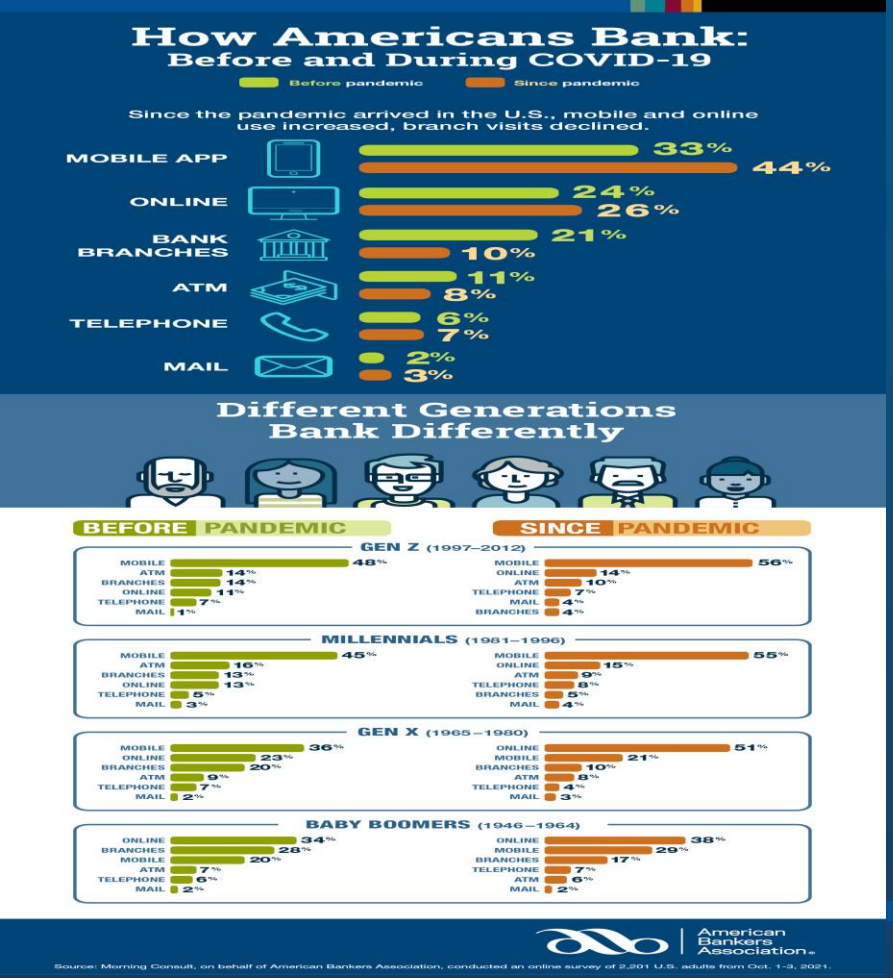


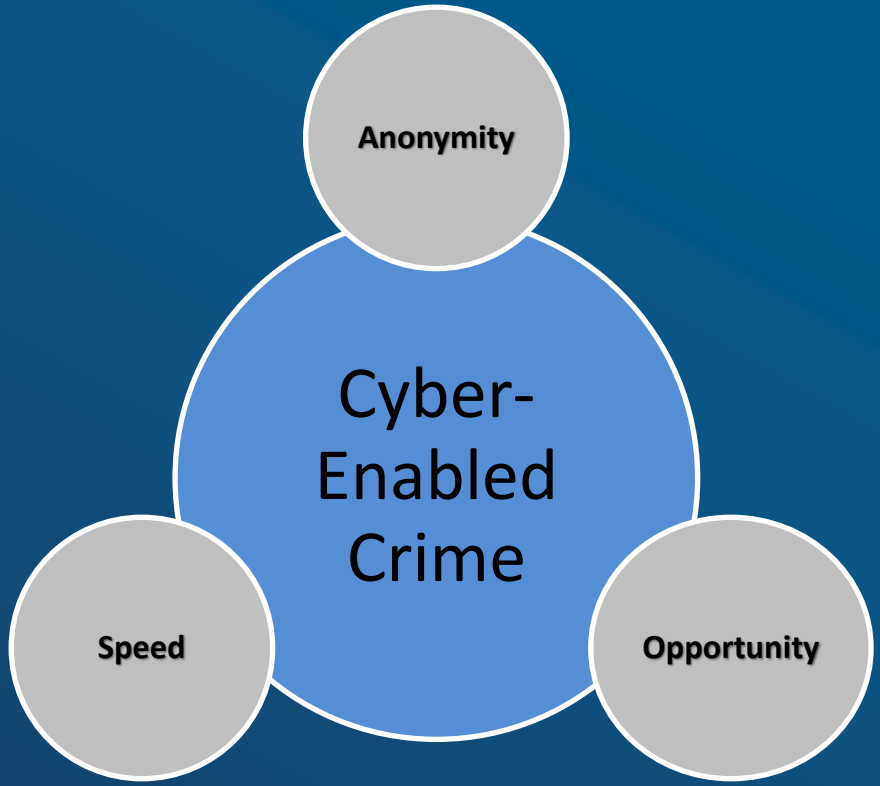
	1q16	2q16	3q16	4q16	1q17	2q17	3q17	4q17	1q18	2q18	3q18	4q18	1q19	2q19	3q19	4q19	1q20	2q20	3q20	4q20	1q21	2q21
ACH	7,512	8,119	6,174	3,757	3,337	3,906	2,953	3,297	4,833	4,550	2,337	2,906	2,658	12,617	5,936	6,393	14,118	25,122	112,00	54,449	32,171	23,390
Wire	1,305	1,822	1,418	1,194	1,362	987	1,225	1,420	2,159	3,633	1,527	2,077	2,334	1,962	2,136	1,845	2,005	3,583	3,419	3,019	3,691	3,186
Billpay	5,523	5,190	5,396	3,573	3,833	3,764	4,559	3,918	3,902	4,690	5,622	4,751	4,473	4,443	3,090	2,822	3,523	3,286	6,225	4,032	1,782	1,979
Count	10	10	9	7	9	8	7	7	7	5	4	4	5	5	4	4	6	6	7	6	6	5

Distribution of Fraudulent Transactions Based on Amount in $ Thousands



	1q16	2q16	3q16	4q16	1q17	2q17	3q17	4q17	1q18	2q18	3q18	4q18	1q19	2q19	3q19	4q19	1q20	2q20	3q20	4q20	1q21	2q21
ACH	144,54	41,546	34,573	27,678	13,661	2,138	1,537	6,569	2,740	2,335	1,323	1,852	2,551	6,048	2,043	2,536	6,765	25,511	81,046	40,427	25,242	18,440
Wire	10,011	11,806	10,589	11,212	22,949	10,061	6,083	7,796	6,683	9,004	7,803	9,346	10,994	8,760	8,680	7,998	8,641	14,321	29,351	21,786	44,180	28,006
Billpay	14,206	13,637	21,001	11,210	13,511	12,566	14,350	12,874	15,059	23,344	28,801	19,703	16,849	18,354	9,777	10,482	13,312	20,070	11,877	7,056	8,134	6,216
Count	10	9	9	7	9	8	7	7	7	5	4	4	5	5	4	4	6	6	7	6	6	5


How Americans Bank:
Before and During COVID-19
Before pandemic
Since pandemic
Since the pandemic arrived in the U.S., mobile and online use increased, branch visits declined.
MOBILE APP 33% 44%
ONLINE 24% 26%
BANK BRANCHES 21% 10%
ATM 11% 8%
TELEPHONE 6% 7%
MAIL 2% 3%
Different Generations Bank Differently
BEFORE PANDEMIC
SINCE PANDEMIC
GEN Z (1997–2012)
MOBILE 48% ATM 14% BRANCHES 14% ONLINE 11% TELEPHONE 7% MAIL 1%
MOBILE 56% ONLINE 14% ATM 10% TELEPHONE 7% MAIL 4% BRANCHES 4%
MILLENNIALS (1981–1996)
MOBILE 45% ATM 16% BRANCHES 13% ONLINE 13% TELEPHONE 5% MAIL 3%
MOBILE 55% ONLINE 15% ATM 9% TELEPHONE 8% BRANCHES 5% MAIL 4%
GEN X (1965–1980)
MOBILE 36% ONLINE 23% BRANCHES 20% ATM 9% TELEPHONE 7% MAIL 2%
ONLINE 51% MOBILE 21% BRANCHES 10% ATM 8% TELEPHONE 4% MAIL 3%
BABY BOOMERS (1946–1964)
ONLINE 34% BRANCHES 28% MOBILE 20% ATM 7% TELEPHONE 6% MAIL 2%
ONLINE 38% MOBILE 29% BRANCHES 17% TELEPHONE 7% ATM 6% MAIL 2%
American Bankers Association
Source: Morning Consult, on behalf of American Bankers Association, conducted an online survey of 2,201 U.S. adults from Oct. 1-3, 2021.


Anonymity
Cyber-Enabled Crime
Speed
Opportunity

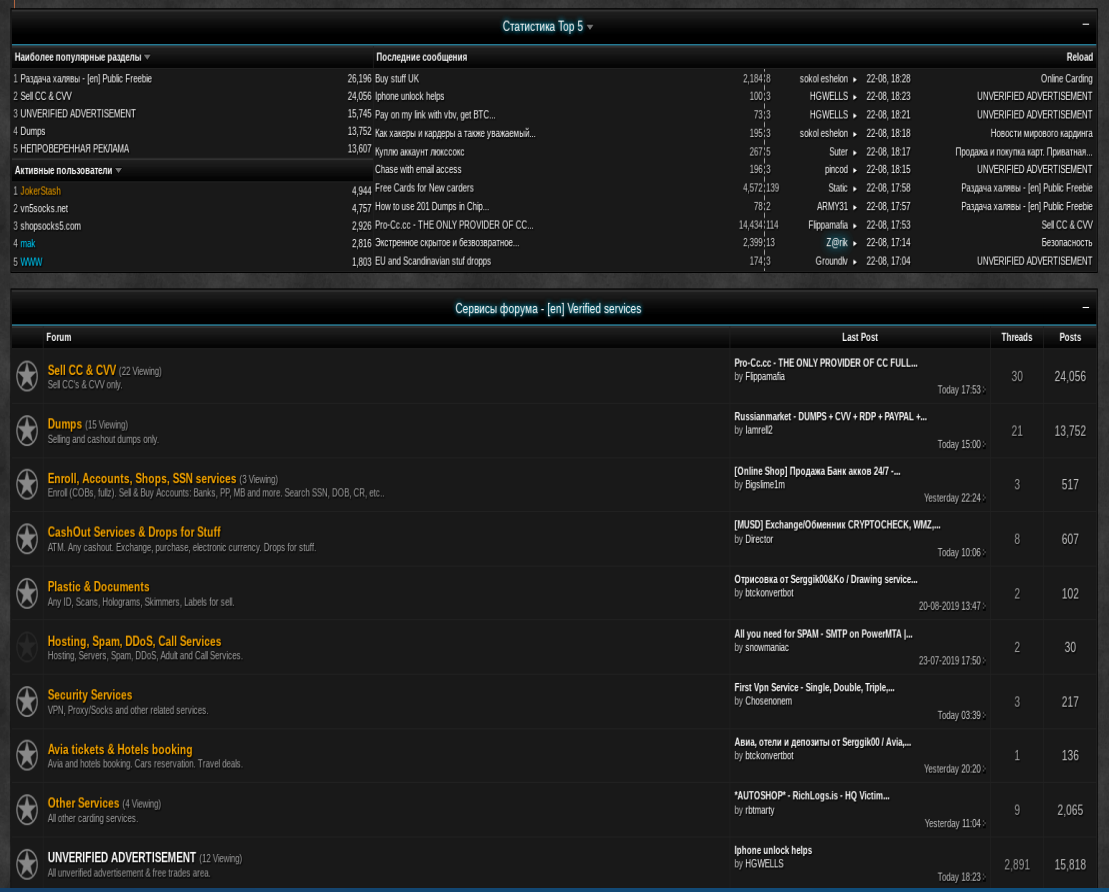
Cyber Enables…

Today's Banking Paradigm

…Cyber Enables…

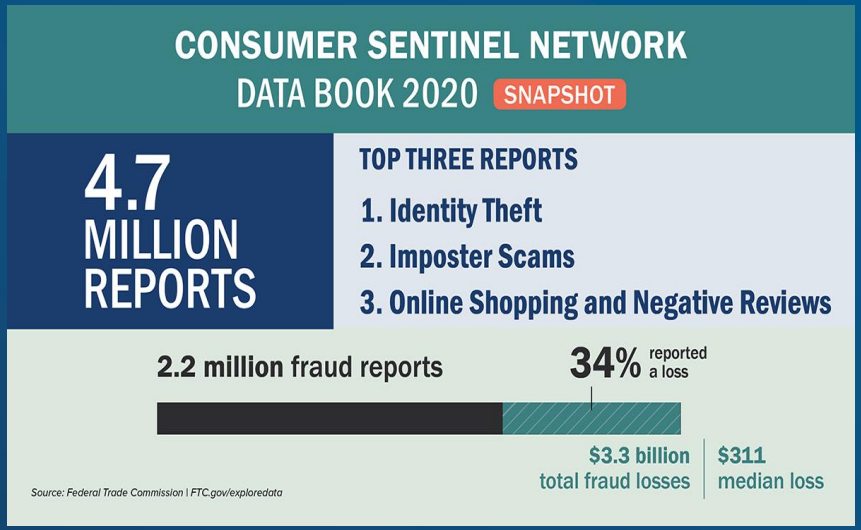
Dark Market/Web Forum

- Anonymous interaction using TOR
  - Phishing kits
  - Credential Stuffing packages
  - “Credit Card number sells for $2 on the black market while a health record goes for $20 or more…”
    -Peter B. Nichol, PMP, CSSMBB
  - “Social Security Number sells for $1.00 and a drivers license $20…”
    -FiVerity
  - Cashout/Mule Services



…But People “Facilitate” Fraud.

- 30% of people surveyed use same password for financial accounts as other account(s) – *CSI 2021 Consumer Survey*
- Every day people fall victim to fraudulent calls, texts and emails pretending to be their bank
- Nothing is free in life, beware of online job offers “working from home, moving money”



MO of a Fraud Scam

- Uses phone call, text or email
- Pretends to be in a position of trust
  - Family member/acquaintance
  - Government official
  - Banker fixing account
- Sets a sense of urgency
- Requests personal information
- Requests money using wire, gift card or cryptocurrency

Best Defense: DO NOT TRUST until verified

Go on Offense…Educate Employees and Consumers!

- Stay current on threats
  - FinCEN Advisories
  - Associations
  - LE Working Groups
- Engaging content
- Consider frequency
  - Spread anti-fraud/cyber training throughout the year
- Test behavior
  - Sandboxed phishing emails

Stay on Offense…Your E-Device is a Connected Treasure Trove

- Primary way attackers compromise computers is through viruses that exploit vulnerabilities on devices
- A device that has the latest security updates to its OS and apps may still be at risk
  - undetected flaws and RDP vulnerabilities
- Devices can become infected by seemingly innocent outside sources such as e-mail, flash drives, and web downloads
  - Continuously updated protection against exploits. Anti-virus software is a must
  - 2 Factor Authentication
  - STRONG password requirements, requiring regular resets

State Unemployment Insurance Fraud

Enhanced benefits made this more attractive to criminals

Overburdened state agencies prioritized making payments

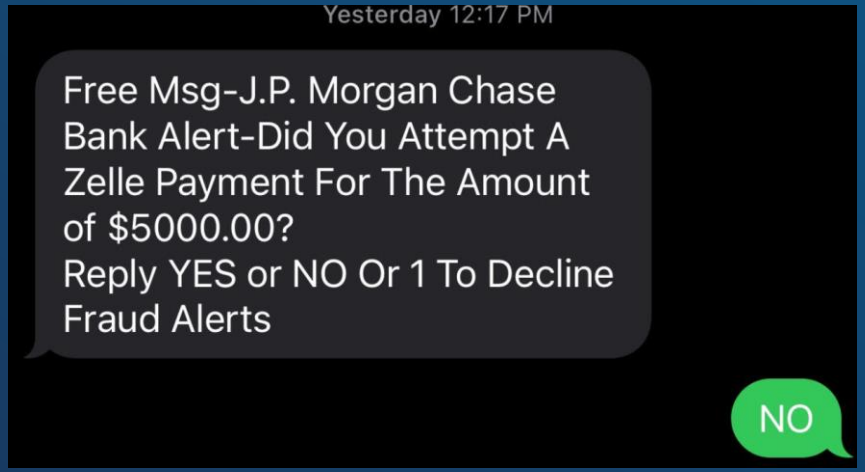
State online systems did not have adequate identify fraud safeguards

Red flags

- Account receives UI payout from out of state.
- Account receives multiple UI payments from different states
- Account receives multiple UI payments under different names.
- Account makes outgoing payments immediately upon receipt.

Simple, Fast Payment Process, into ID Theft or Mule Accounts

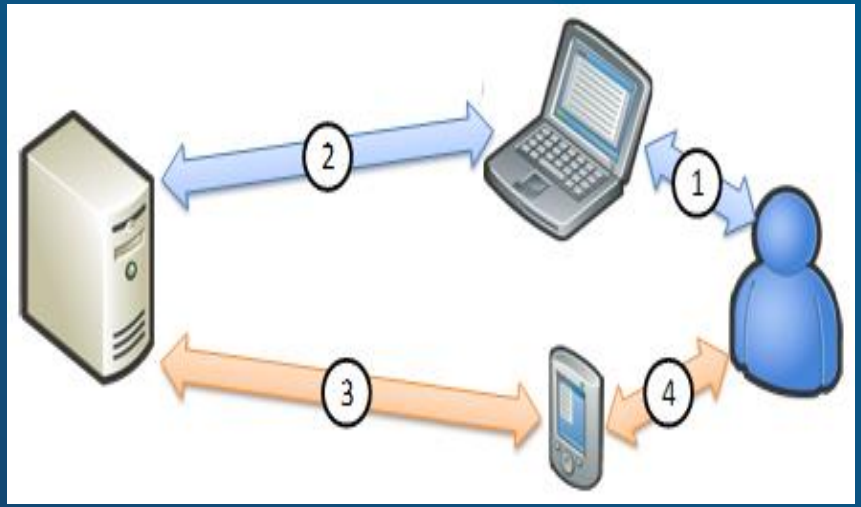
P2P - Zelle Fraud



- After victim responds (yes or no), fraudster calls them
- Fraudster socializes username and initiates password change
  - To defeat 2 step auth, fraudster keeps victim on phone and gets passcode to change password
- Password is changed and P2P payments are made to fraudsters accounts

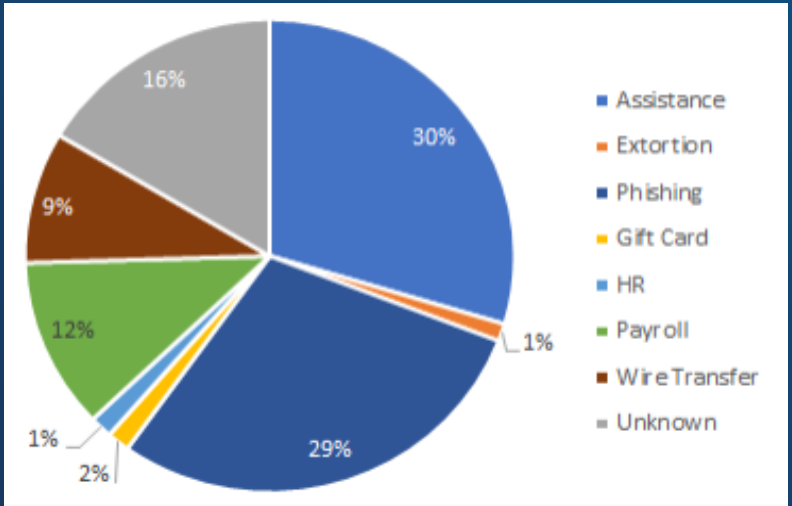
P2P Fraud Defense

- 2 factor authentication
  - Resets with OTP using out of band authentication
- Real time activity monitoring based on account behavior (like credit card models/rules)
  - Geolocation
  - Spending pattern
- Block auto enrollment of P2P
  - Require customer to initiate via verification process, and educate them
- Educate to NOT Trust until VERIFIED
  - Hang up and call bank directly, for ex.



How Email Compromise Fraud (BEC / EAC) Works & Common Themes

Most Common – “CEO Assistance”



Step 1: Identifying the Target

Malicious actors target a business or bank, exploit available online information and develop a profile of the company and its executives.

Step 2: Preparing the Target

The actors use phishing or telephone social engineering methods and contact company personnel. (typically someone in finance)

The employee is manipulated by exploiting human nature; taking days or weeks.

Step 3: Information Exchange

The employee is convinced they are communicating with the executive and performing a legitimate business transaction.

The employee is provided wire transfer instructions to a bank account controlled by the actor.

Step 4: Wire Transfer & Get-a-way

Following the successful wire transfer, the funds are withdrawn, and the actor flees…

Note: The actors may attempt future wire transfer requests.

Best Defense is Training of BEC /EAC "Red Flags"

- ✓ An urgent email requesting that a wire transfer be sent immediately
- ✓ The email domain name is very similar to the legitimate domain
- ✓ The content of the email reflects:
  - ❖ Urgency
  - ❖ The sender is out of the office
  - ❖ Leverages position within the bank
- ✓ The position of the sender

➢ **Teach, Do Not trust until verified**

ABA Tools & Notes

- ABA Initiative: #BanksNeverAskThat Campaign
  - Oct 1, ABA and banks across the country launched a Phishing awareness campaign
  - Campaign includes attention-grabbing, humorous content aimed at empowering consumers to identify bogus bank communications that ask for sensitive information (e.g., passwords & social security numbers)

- Ransomware Toolkit | American Bankers Association (aba.com)

- ABA Reg E Guidance
  - https://www.aba.com/banking-topics/compliance/from-the-hotline/reg-e-dispute-scam
  - https://www.aba.com/banking-topics/compliance/from-the-hotline/reg-e-unauthorized-transaction-claim

- Regulator Notice of Final Rule, November 2021, requiring 36- hour notification of computer security incident (Compliance date: May 1, 2022):
  - Federal Register notice: Computer-Security Incident Notification Requirements for Banking Organizations and Their Bank Service Providers (federalreserve.gov)
  - Staff Analysis: Computer-Security Incident Notification Rule | American Bankers Association (aba.com)

- FFIEC Cyber Risk Assessment Toolkit
  - FFIEC_CAT_May_2017_All_Documents_Combined.pdf

Appendix

- Banks Never Ask That!, ABA Campaign
- Scams, Who’s Liable?
- FinCEN Rapid Recovery Program
- Ransomware, what it is and how it infects.
- MSP vs MSSP

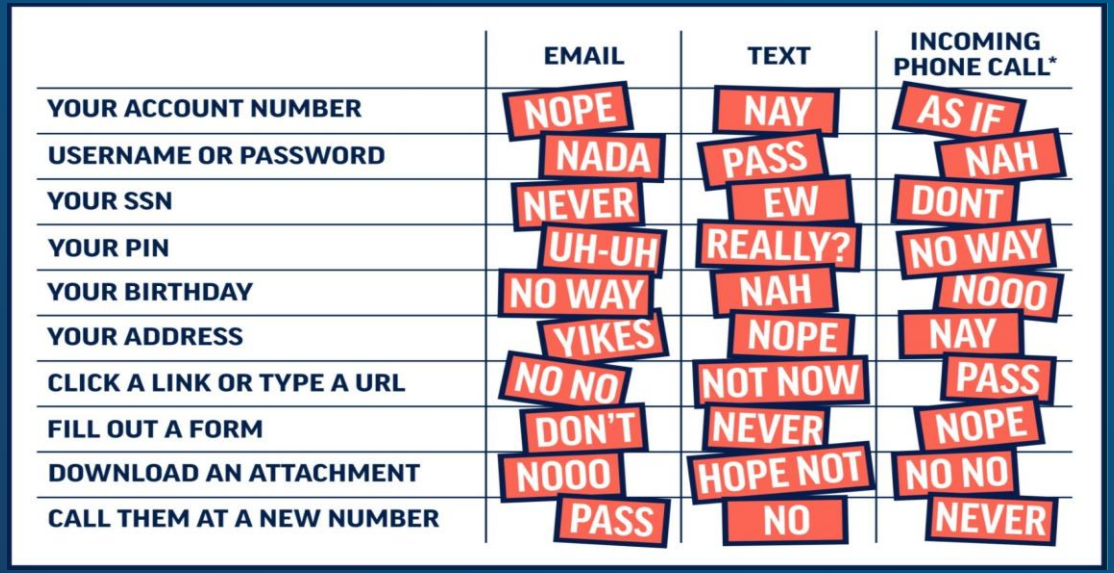
BANKS NEVER ASK THAT

American Bankers Association

Goal:

Continue the success of last year's industry-wide phishing awareness campaign:

Banks Never Ask That! – Every day, people lose hundreds, even thousands of dollars to scammers imitating banks. If a scammer was pretending to be your bank, could you tell the difference?



SCAMS, Who's Liable?

1. The consumer is not liable.

2. Even though the person is being swindled, the consumer would appear to be liable for the amount the consumer agreed to give the fraudster because the consumer gave the fraudster authority to use the access information, much as someone can authorize someone to use their physical debt card.

3. Customer is liable because customer authorized the transaction.

Customer is fraudulently induced to give a fraudster their access information, with no intention that there be a payment (e.g., I am from the bank and you need to verify this information as described in the Bureau's Q&A).

Customer is induced to pay a fraudster as part of a scam and gives bank account access information as a means to pay the fraudster (e.g., passcodes).

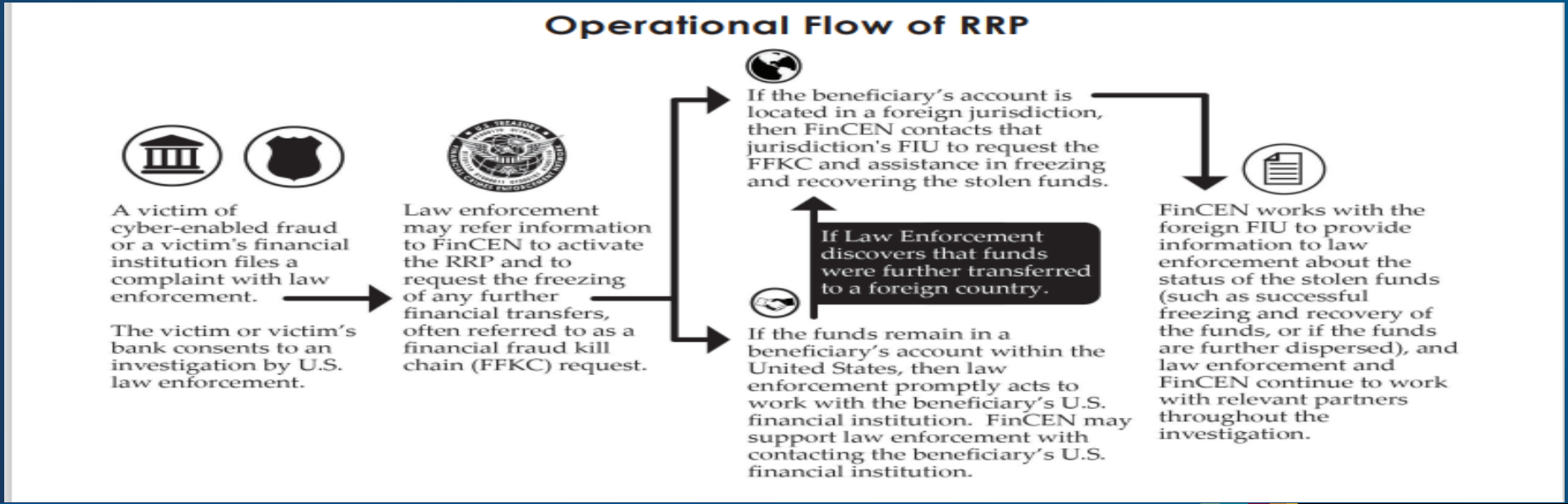
Customer initiates the transaction to pay a fraudster based on a scam e.g., transfers money using Zelle.

*This is an exercise to drive thought and discussion, not legal advice. Seek advice from your legal department when determining liability.

FinCEN Rapid Recovery Program

*Click link for additional details & instructions on how to initiate

RRP Fact Sheet Notice FINAL 508.pdf

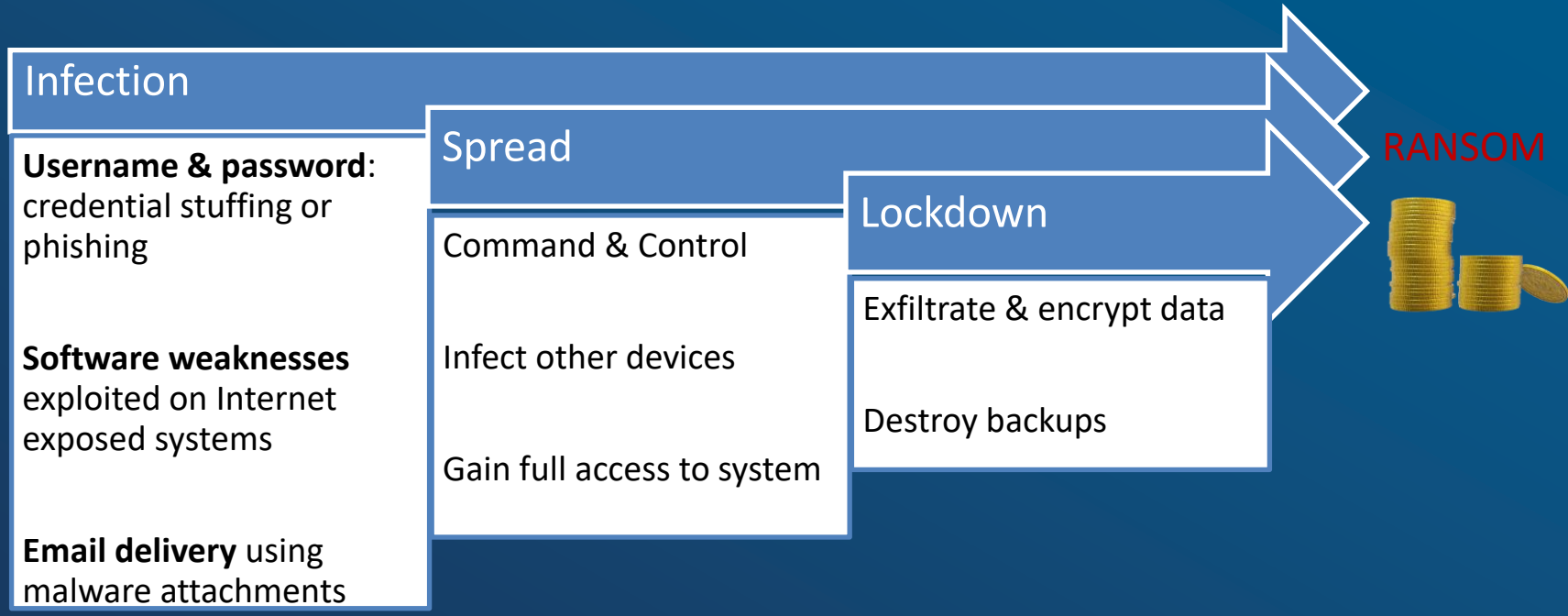


Ransomware – What is it?

Ransomware event occurs whenever a financial institution identifies cyber actors' use of malicious software code ("malware") to encrypt computer systems or stored data, and demands a ransom payment, normally in digital currency (Bitcoin), in exchange to decrypt the systems/data.

Ransomware is the ***result*** of common cyberattacks (DDOS, Phishing, password attack) and security vulnerabilities (unpatched software, RDP attacks), not the cause.

Attack Runs ~90-100 days from Infection to Lockdown



Know the difference between MSP vs MSSP and consider a layered approach

Managed Service Provider

- Provides information system availability to employees & customers
- Primarily focused on administration of network
  - IT roadmap
  - Data backup
- Engaged for usability and performance
  - Help Desk

Managed Security Service Provider

- Protects information systems from outside users
- Primary focus if IT security
  - Scanning, vulnerability patching, user authentication
- Detects & responds to threats across IT infrastructure
- Align security with compliance frameworks

Jim Hitchcock, VP Fraud Mitigation

jhitchcock@aba.com