



Cyber Financial Crime Victimization




Presented by
Katelyn Wan Fei Ma

 **HARVARD Kennedy School**
JOHN F. KENNEDY SCHOOL OF GOVERNMENT

Science and Democracy Network 22nd Annual Meeting
August 24-26, 2023
Harvard Kennedy School
79 John F. Kennedy Street, Cambridge, MA

 **BUDAPEST CONVENTION ON CYBERCRIME**
OF THE COUNCIL OF EUROPE
CONVENTION DE BUDAPEST SUR LA CYBERCRIMINALITÉ
DU CONSEIL DE L'EUROPE

20+ SINCE 2001  COUNCIL OF EUROPE
CONSEIL DE L'EUROPE



Ph.D Candidate @ Graduate Program
in Science and Technology Studies
York University



Lecturer, Department of Criminology,
Faculty of Human and Social
Sciences, Wilfrid Laurier University



Manager of Strategic Initiatives, North
American Fraud Operations

Topic Covered Today



- Introduction
 - What's Cyber Financial Crime
 - Science and Technology Studies (STS)
 - STS Concepts
- My Academic & Professional Experience... So Far
- COVID & Cyber Financial Crime: Typology
- Re – Defining Cyber Financial Crime Victimization: Financial Institutions
- Q&A

INTRODUCTION

#Cybercrime

Action directed against the confidentiality, integrity and availability of computer systems, networks and computer data (Council of Europe, 2001).

**\$1.5 TRILLION
DOLLARS**

**\$9 TRILLION
DOLLARS**

2018

2025

(United Nations,
2022)



#CyberFinancialCrime

A subset of cybercrime - often referred to as technological crime involving the unlawful possession of property belonging to others

Most cyber financial crime cases result in (or attempt to result in) monetary loss as the unauthorized users often attempt financial gains through technological exploitation

What's Science and Technology Studies?

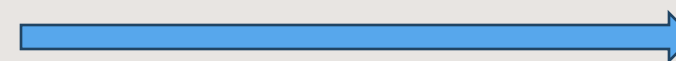
Scientific knowledge is collectively produced, constituted and legitimated

Pay attention to both the social and the material context

Technoscience = socially and culturally configured and is not free from social bias and prejudice

Lay expertise and citizen science can also be valid when considering both technoscientific and political actions and choices

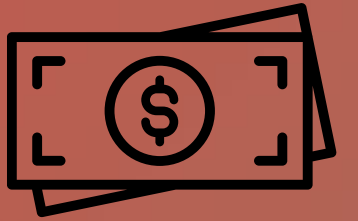
Technoscience and society are often co-produced in that our social orders are shaped by technoscience and vice versa



STS Concepts

Victimization
Punishment
Public-Private
Laws
Regulations
Non-Human
Sociotechnical Imaginaries
Performativity
Financial
Transparency
Technology
Data
Expertise
Development
Unboxing
Algorithm
Fairness
Democracy
Trust
Transfer
Co-production
Rules
Boundaries
Interpretation
Artificial Intelligence
Voice
Partnership
Framing
Use
Procedure
Crime
Knowledge
Misuse
Actor
Social Construction
Accountability
Reflexivity

Why not Criminology / Information Security



- Contested Definition
- Situated knowledge: financial institutions have the situated knowledge to make situated claims, and therefore produce situated legitimacy
- A part of “knowing” is also knowing how to “work the system”—how to make consumers acknowledge their misconduct and how to shape their victimization experiences based on each case scenario
- Criminology is often binary – but cybercrime/cyber financial crime is often not

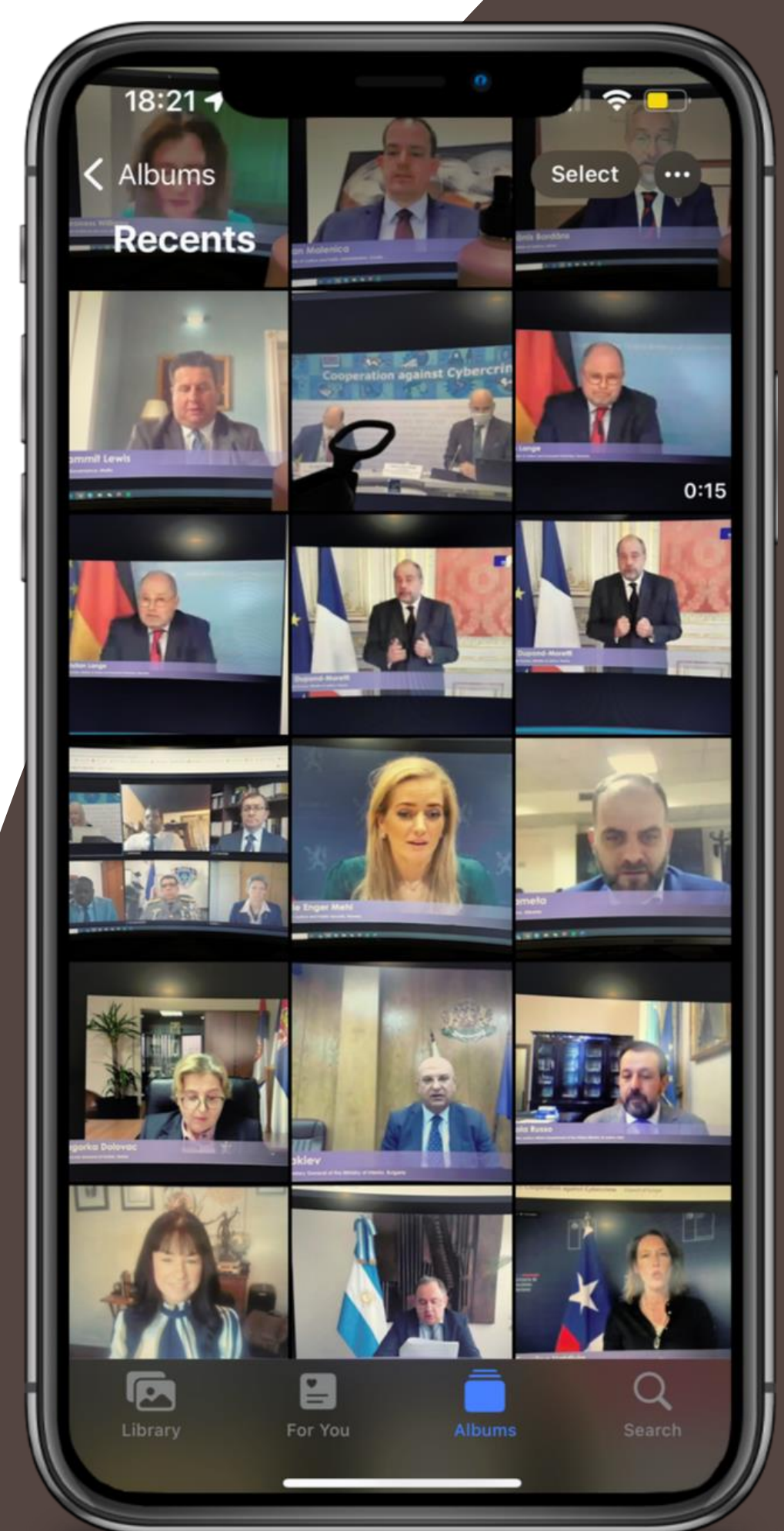


How do we create a democratic and scientific governance process when financial institutions are the only actors that have access to privileged situated knowledge?





Council of Europe Octopus Conference 2021





Octopus Conference 2021

Lightning Talk: Participatory Governance: Co-Creating Cyber Fraud Management Knowledge

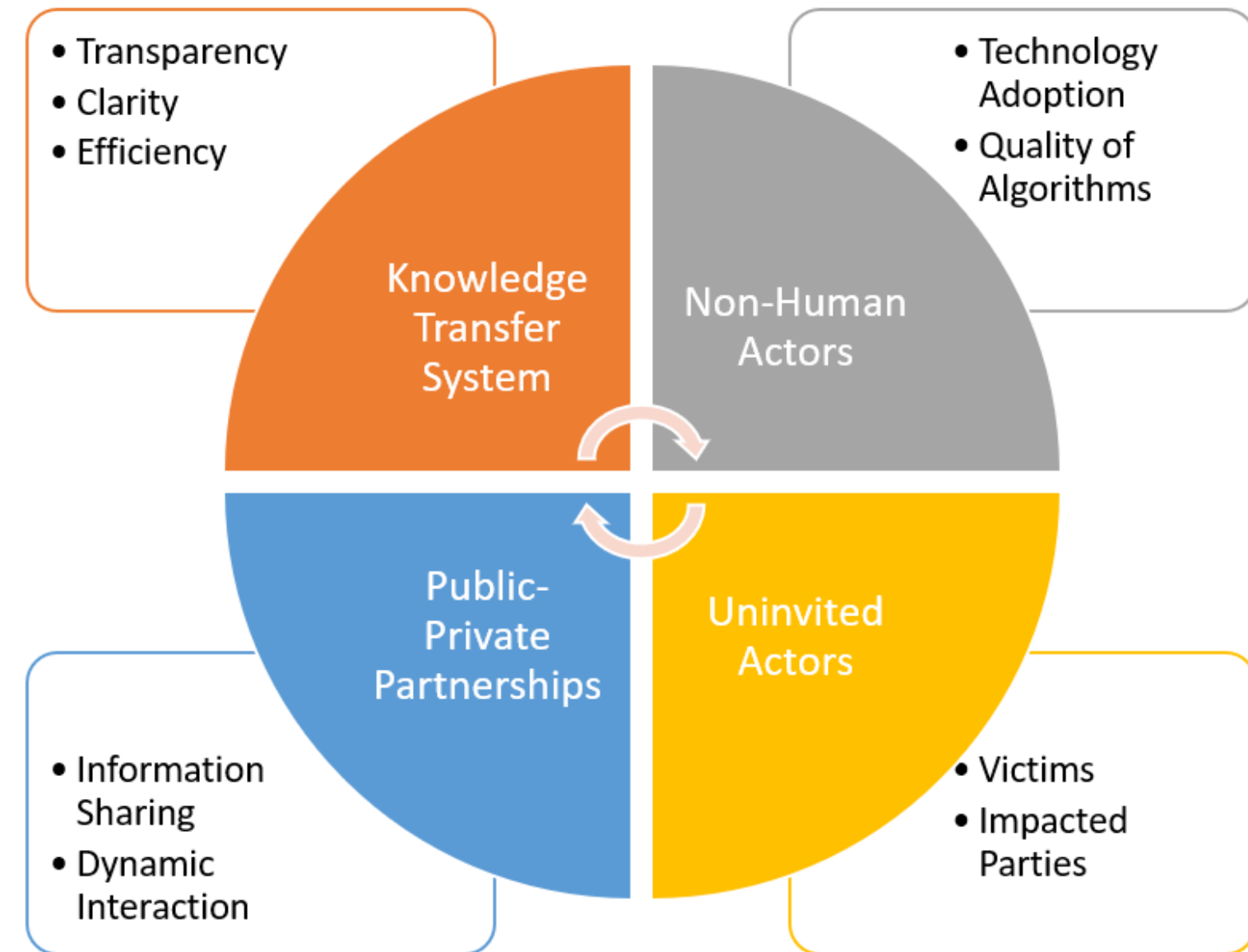


Katelyn Wan Fei Ma



Cybercrime PhD Candidate, York University
Horizontal Fraud Strategist, TD Bank

- **Cyber Fraud Trends:** Creative and Unpredictable
- **Broken Trust:** Technological and Institutional
- **Build and Rebuild Trust:** Participatory Governance
- **Co-Creating Knowledge:**
 - Non-Human Actors
 - Uninvited Actors
 - Public-Private Partnerships
 - Knowledge Transfer System
- Highlighting Democracy and Sustainability

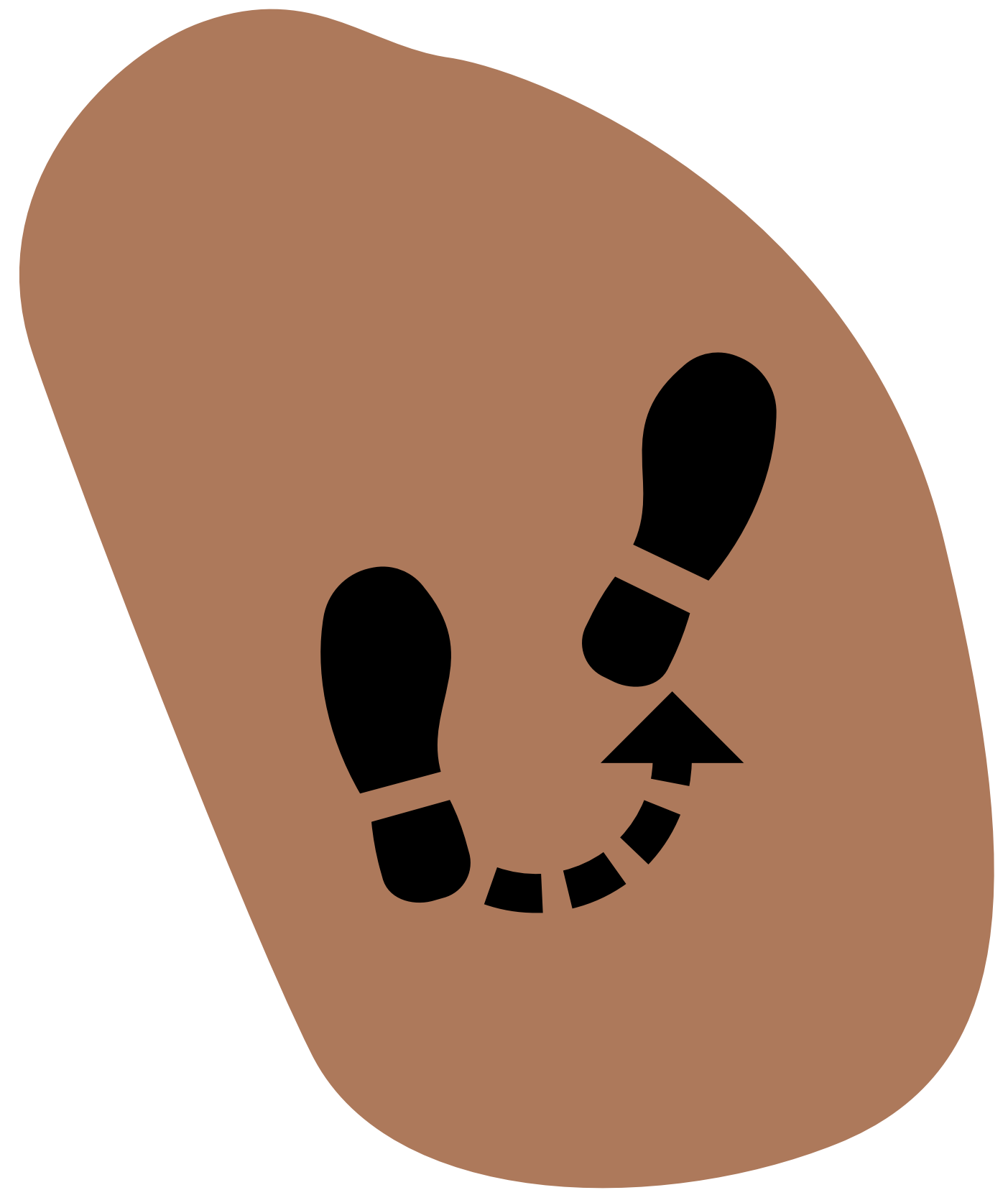


Trust = Democratic Technology and Governance Environment + Sustainable Relationship Management



Part Two

My Academic &
Professional
Experience... So Far

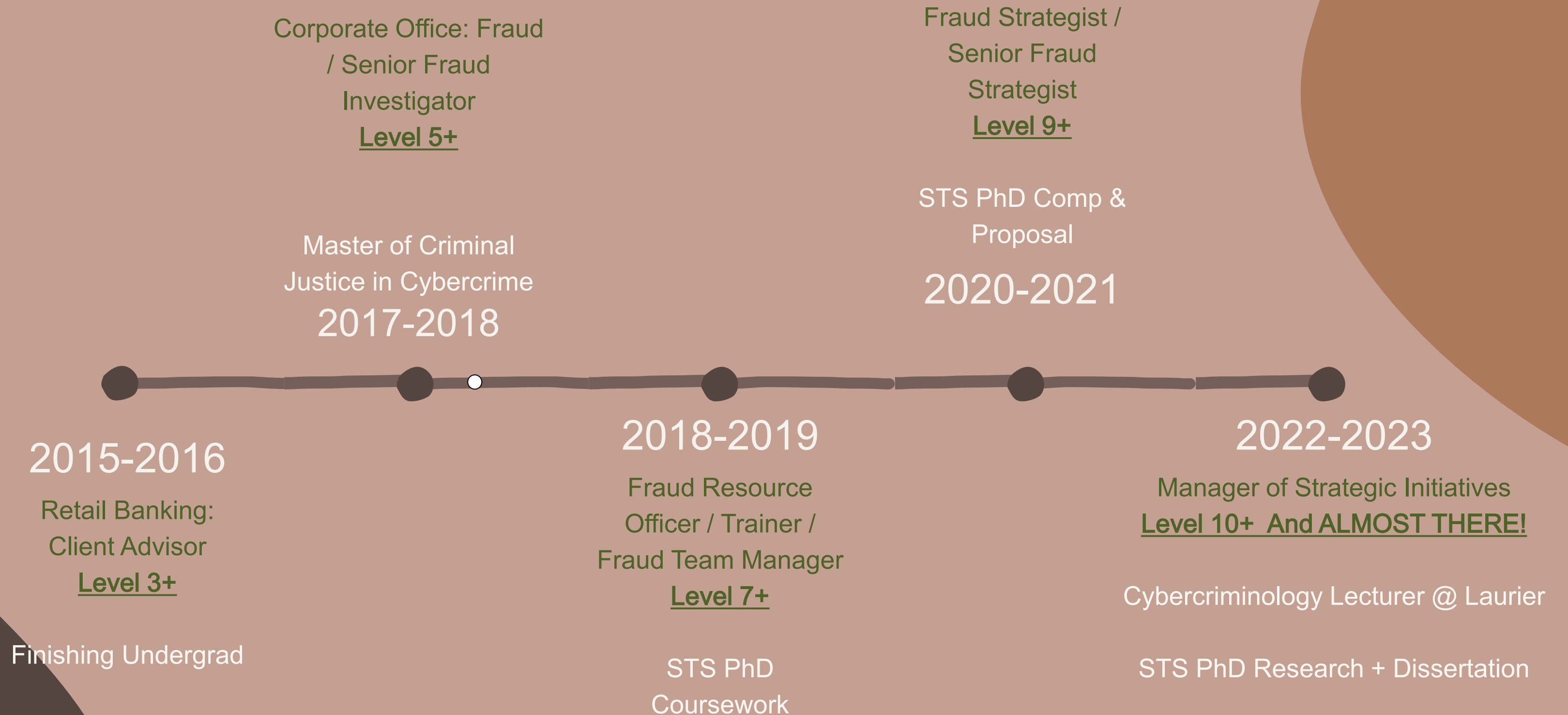


Student Question:

What it takes and what it needs to become a cyber security worker in a bank. What does the career path look like?

My Career/PhD Journey

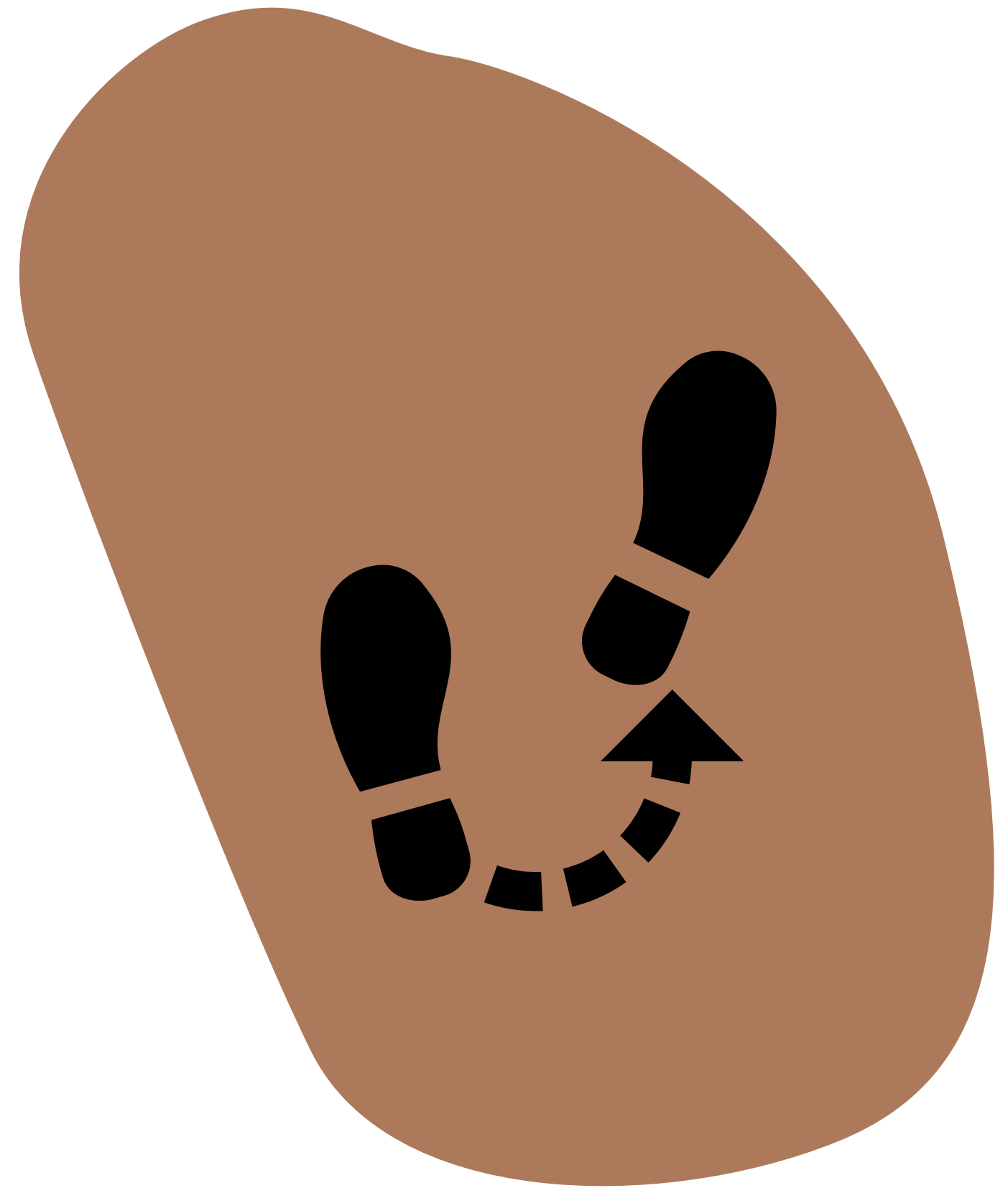
Learning and Growing





Part Three

COVID & Cyber Financial Crime: Typology



About COVID-19 & Cyber Fraud

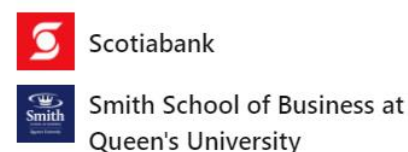
As the public moves from **in-person to online** activities, the likelihood of cybercrime victimization also increases.

Cybercriminals now have more opportunities to exploit online service users in various creative ways.

Ma, K. W. F., & McKinnon, T. (2021). COVID-19 and cyber fraud: emerging threats during the pandemic. *Journal of Financial Crime*.



Tammy McKinnon · 1st
SVP, Global Fraud Management at Scotiabank
Toronto, Ontario, Canada · [Contact info](#)



The current issue and full text archive of this journal is available on Emerald Insight at:
<https://www.emerald.com/insight/1359-0790.htm>

COVID-19 and cyber fraud: emerging threats during the pandemic

COVID-19 and
cyber fraud

Katelyn Wan Fei Ma

Department of Science and Technology Studies, York University, Toronto, Canada, and

Tammy McKinnon

Queen's University, Kingston, Canada

Abstract

Purpose – The emergence of the novel coronavirus (COVID-19) has threatened physical and mental health, and changed the behaviour and decision-making processes of individuals, organisations, and institutions worldwide. As many services move online due to the pandemic, COVID-19-themed cyber fraud is also growing. This article explores cyber fraud victimization and cyber security threats during COVID-19 using psychological and traditional criminological theories. It also provides a COVID-19-themed cyber fraud typology using empirical evidence from institutional and agency reports. Through organizing COVID-19-themed cyber fraud into four different categorizations, we aim to offer classification insights to researchers and industry professionals so that stakeholders can effectively manage emerging cyber fraud risks in our current pandemic.

Design/methodology/approach – The approach the study take for this conceptual paper is typology.

Keywords Financial crime, Cybercrime, Scams, Cyber security, COVID-19, Cyber fraud, Infodemic, Pandemic, Policing

Paper type General review

61%
of Canadian's surveyed say that social isolation can increase vulnerability to fraudsters.



TD Bank Group
Newsroom

Receive TD News Alerts

Right after COVID

Canadians cite strong connection between social isolation and vulnerability to fraud - but the truth is, everyone is vulnerable

- Majority of Canadians (61%) say that social isolation can increase vulnerability to fraudsters
- Canadians also believe various major life changes increase one's vulnerability to fraud
- Boomers seen as most at risk (71%) by other generations; but Canadians between the ages of 56 and 76 are the most likely to state that they personally do not feel vulnerable (92%)

TORONTO, March 3, 2020 /CNW/ - According to a TD Fraud Survey released today for Fraud Prevention Month, a majority of Canadians believe social isolation and major life changes increase Canadians' vulnerability to financial fraud. While fraudsters continue to target Canadians of all ages and life stages, only 13% of Canadians say they personally feel vulnerable about being a target for fraud.

"Fraudsters don't discriminate; they target Canadians of all ages and stages of life and absolutely nobody is immune to being targeted by a fraudster," said Tammy McKinnon, Head of the Financial Crimes & Fraud Management Group at TD. "While going through major life changes or being socially isolated can contribute to heightened vulnerability to fraudsters, it's vital that all Canadians stay vigilant, be aware of common scams, and familiarize themselves with ways to avoid falling victim to fraud."

Life stage can impact vulnerability

Canadians surveyed also believe major life changes can play a role in how vulnerable someone may be to fraud. Key life changes seen to make people more vulnerable to fraudsters include:

- Moving to Canada from another country (35%) – unfamiliarity with Canadian banking, tax, or legal practices may lead to increase susceptibility to fraud attacks like the CRA scam
- Recent death in the family (32%) – those coping with loss may be more likely to fall for an emergency scam, if they believe a family member needs help
- A recent divorce or separation (25%) – starting to date after the end of relationship may lead to increased susceptibility to a romance scam
- Moving away from home for the first time (i.e. to attend university or college) (20%) – those who are new to managing their own budget/finances fall prey to common phishing, text message or email scams
- Starting a new job (9%) – first time job seekers may be more likely to fall prey to an employment scam

How Canadians perceive fraud risk

Survey results also found a strong disconnect between how generational groups feel about themselves personally and how they are perceived by others when it comes to vulnerability to fraud. Gen Z or students (29%) and Millennials (16%) are the most likely age groups to feel they are vulnerable or a target while Boomers (92%) are the most likely to *not* feel personally vulnerable.

Cyberfraud Soars During Pandemic: 'New Wine in Old Bottles'

By Nancy Bilyeau | November 9, 2020

LIKE TWEET EMAIL PRINT MORE



Numerous so-called "cures" for the coronavirus like this one are being sold openly over the Internet. Photo courtesy U.S. Food and Drug Administration via Flickr

More than 223,000 COVID-19-related online fraud or scam claims have been received by the U.S. Federal Trade Commission as of October 21, according to a new paper.

Estimated losses to that date were over \$160 million, reported the paper, entitled "COVID-19 and Cyber Fraud: Emerging Threats During the Pandemic."

"Current academic research and industry reports have shown that fraudsters have put old wines into new bottles to defraud targeted victims by abusing the COVID-19 context," said the authors, Katelyn Wan Fei Ma of York University and Tammy McKinnon of Queen's University, both in the Canadian province of Ontario.

The paper, which has not yet been peer-reviewed, argued that as COVID-19 forces people to work, shop and interact with friends and loved ones online, cybercriminals are finding many more opportunities to exploit all these online service users.

"As the public moves from in-person to online activities, the likelihood of cybercrime victimization also increases, which may result in a disruption of services, financial loss, data breaches, and individual and institutional anxieties," the authors wrote.

You are here: Cybercrime > Octopus Conference > Octopus conference 2021

Lightning talks

Due to the ongoing Covid-19 pandemic, the Octopus Conference 2021 will be a 100% online event. The Lightning talks will be held on 17 and 18 November 2021.

Deadline for submission of proposals was 1 November 2021, 10:00 AM Strasbourg time.

We would like to thank everyone who submitted their idea and for their willingness to share it with the community.

What is the format?

- video conference platform
- 1 slide only
- Duration of presentation 6 minutes
- 4 minutes Q&A from the public.
- Presentation languages; English, French, Spanish and Portuguese

This year's selected speakers and their ideas:

TALKS

<p>Isabella Wilkinson Research Associate, International Security Programme, Chatham House</p> <p>Strengthening Effective and Inclusive Cybercrime Policymaking</p>	<p>Katherine Quezada Tavaréz Researcher, KU Leuven Centre for IT & IP law (CITIP)</p> <p>Legal Challenges in Bringing AI Evidence to the Criminal Courtroom</p>	<p>Roberto Roman Contreras Comandante del Departamento de Crímenes y Delitos de Alta Tecnología, Policía Nacional, República Dominicana</p> <p>Triangulo del Delito</p>
<p>Ilvana Dedja Graduate law student, Queen Mary University of London</p> <p>A human in the Matrix: One step closer to 1984</p>	<p>Anna Katariina - Ovaska Legal specialist, global criminal lawyer, Protect Children/Suojellaan Lapsia ry. NGO Helsinki, Finland</p> <p>Global Collaboration Against Global Crime - Protecting Children from Sexual Violence</p>	<p>Pablo López-Aguilar Director of Technology Anti-Phishing Working Group - Europe (APWG.EU)</p> <p>An Effective Approach to the Cross-Border Exchange of Digital Evidence Using Blockchain</p>
<p>Oluwatosin Falebita Second-in-command IITA Police Station, Nigeria Police Force</p> <p>A call to action on digital privacy and freedom</p>	<p>Roberto Contreras Senior Advisory Lawyer, former Cybercrime Prosecutor at the Public Ministry of Chile</p> <p>Artificial intelligence in the criminal justice system. Neuro-rights and Cybercrime.</p>	<p>Katelyn Wan Fei Ma PhD Candidate (York University Cybercrime), Horizontal Fraud Strategist (TD Bank)</p> <p>Co-creating a diverse cyber fraud management knowledge base</p>

← → ↻ 🏠 scamalert.sg

SCAM ALERT
BRINGING YOU THE LATEST SCAM INFO

Types of Scams ▾ Stories Media News Resources ▾ Let's Fight Scams [Share a Story](#) English ▾

ANTI-SCAM HELPLINE:
1800-722-6688
(Mon – Fri, 9am – 5pm, excl. PHs)

Blog
Building Societal Resilience to Scams eBook
Posters
Videos
You Got Scammed, What's Next?

SURE OR NOT?

Do not commit too quickly.
Consider the risks before you do.

[Find Out More](#)

Facebook Instagram YouTube WhatsApp Print

SCAMMER, BEWARE:
BUILDING SOCIETAL RESILIENCE TO SCAMS
A Behavioural Sciences Perspective
Results of the National Prevalence Survey of Scams 2020

Home Team Behavioural Sciences Centre
Crime, Investigation and Forensic Psychology Branch

FOREWORD

Minister of State Mr Desmond Tan's Message

Scams are a grave issue. In the past five years, the number of reported scam cases and amount lost to scams have tripled.

In 2020 alone, scams accounted for 42% of all crime in Singapore with losses estimated at SGD 265 million. In 2021, the largest sum cheated in a single case of a China officials impersonation scam was SGD 6.2 million. Many victims have lost a large part of their retirement savings to scams.



But it is not just about monies lost. Victims of scams may become depressed, with some who even considered taking their life after falling victim to scams.

Government agencies, private industries and the community have to work together closely, to arrest the trend of rising number of scams. Since 2020, the government has set up the Inter-Ministry Committee of Scams (IMCS). The IMCS has different government agencies such as the Ministry of Home Affairs, the Singapore Police Force, the Cyber Security Agency of Singapore, the Infocomm Media Development Authority, the Ministry of Communications and Information, the Ministry of Trade and Industry, and the Monetary Authority of Singapore, to coordinate the Government's anti-scam efforts. We work with the private industry too.

The IMCS adopts a multi-pronged approach to tackle scams.

- **Strengthening enforcement.** We have set up specialised units in the Singapore Police Force (SPF) to disrupt scammers' operations, such as the E-Commerce Fraud Enforcement and Coordination Team to tackle e-commerce scams and the Anti-Scam Centre to serve as the nerve centre for investigations into scam-related crimes. The SPF has also stepped up collaboration and conducted joint operations with foreign law

FOREWORD

- **Partnering stakeholders to combat scams.** In addition to drawing on the expertise and resources across Government to combat scams, we also work closely with private sector stakeholders such as banks, digital platforms and telecommunications companies to disrupt scams. For example, SPF works with financial institutions to swiftly freeze bank accounts suspected to be involved in scammers' operations and to weed out money mules. SPF also established close working relationships with telecommunications companies to block spoof calls used by overseas scammers.

- **Public education.** We work with partners such as the National Crime Prevention Council to disseminate advisories through various media platforms, including messaging and social media platforms. We launched our anti-scam public education campaign, "Spot the Signs. Stop the Crimes." in August 2020, focusing on sharing real-life scam examples to educate the public on how to spot the tell-tale signs of various scams.

The best defence against scams is a discerning and vigilant public. Everyone can play a part in stopping scams. Be alert and practice healthy scepticism. Help to raise awareness of scams by talking to your family and friends about scams.

To study the 'DNA' of scams so we disrupt them better, the MHA Home Team Behavioural Sciences Centre (HTBSC) conducted a large-scale research using the National Prevalence Survey of Scams in 2020. The survey yielded information about the behavioural and psychological profiles of scam victims and non-victims. Various inter-government agencies have adopted these findings captured in this report. We hope that this booklet, with its research findings, would be useful for your anti-scam efforts.

Mr Desmond Tan
Minister of State
Ministry of Home Affairs and Ministry of Sustainability and the Environment

THE PANDEMIC-INDUCED CHANGE

The pandemic-induced change from the usual way of everyday life may bring about various sources of added individual stress (Tan & Kurohi, 2020) as societies and individuals alike are posed the challenge of rapid adjustment to the new norms arising from the pandemic (i.e., expedited technological transformation, changes in social interactions). In addition, the presence of COVID-19 as an existential threat may mean individuals are fearful for their economic security, as well as the health and well-being of their loved ones (Baker et al., 2020; Mertens et al., 2020). Consequently, the challenge to adjust and make sense of an uncertain world can be stressful and challenging, such that individuals may experience negative emotions and anxieties, a hyper-vigilant state, and feel inclined to be harm-avoidant in response to a perceived threat from the new lifestyle changes (Taylor, 2019).

Interestingly, many COVID-19-related scams appear to recognise that the added stressors and change due to the pandemic result in individuals becoming more vulnerable targets for crime, as the improvised scam typologies hone in on these heightened emotional vulnerabilities and stressors to target the psychology of potential victims via their fraudulent schemes (Ma & McKinnon, 2021).

In fact, within these uncertain times, the emergence of COVID-19 variants of familiar and novel cybercrime and scams led to an even sharper increase in scams in the last two years. A predictable band of unscrupulous individuals - scammers and cybercriminals - has sought to turn these challenges into opportunities. While crimes involving more physical means have been on the decline (e.g., outrage of modesty cases), cybercrime and scams using virtual means have risen.

Over the past years, reports and advisories from reputable news channels, technology companies, as well as intelligence and enforcement agencies around the world have described new and recycled variants of scams or cybercrime that have surfaced with this



FTC COVID-19 and Stimulus Reports

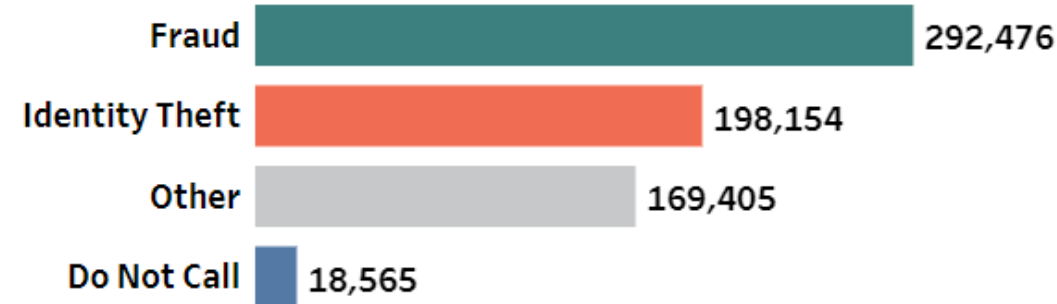
Consumer Sentinel Network Reports

*Data from January 1, 2020 to January 29, 2022

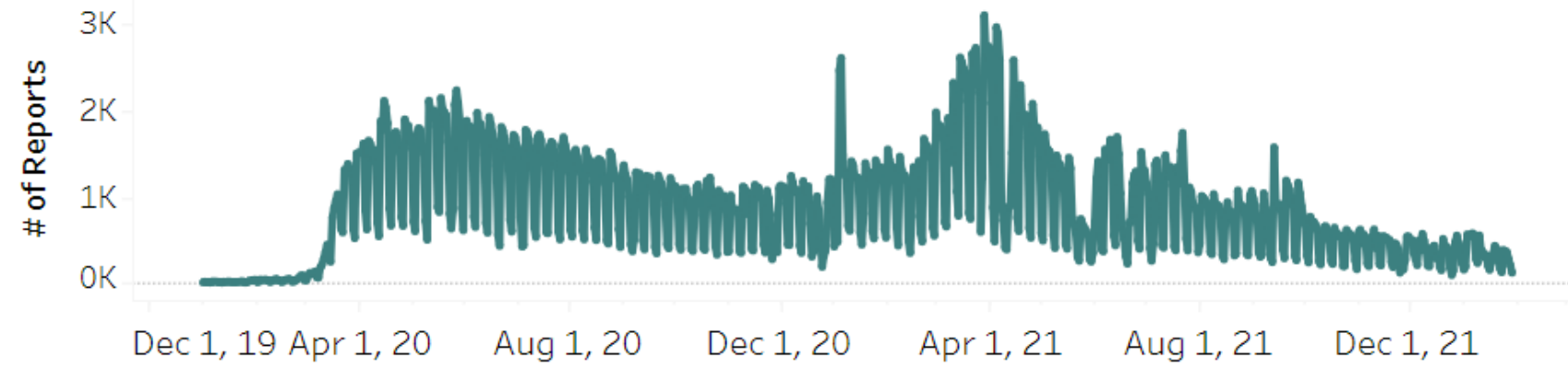
Peak= Spring / Early Summer

By Day

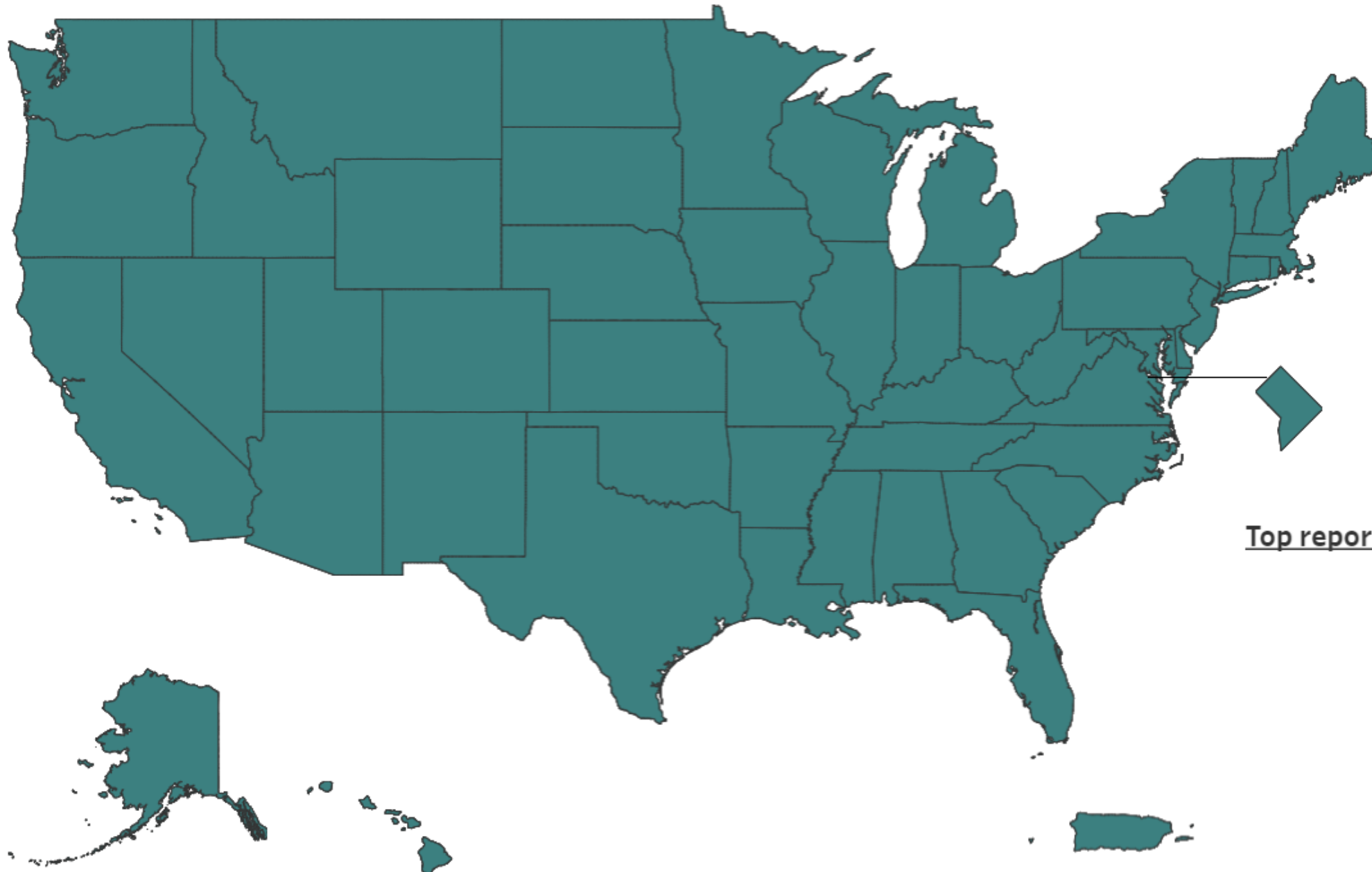
Reports by type: (Select Report Type)



Report trends over time: (Select Time Period)



Reports by state: (Select State)

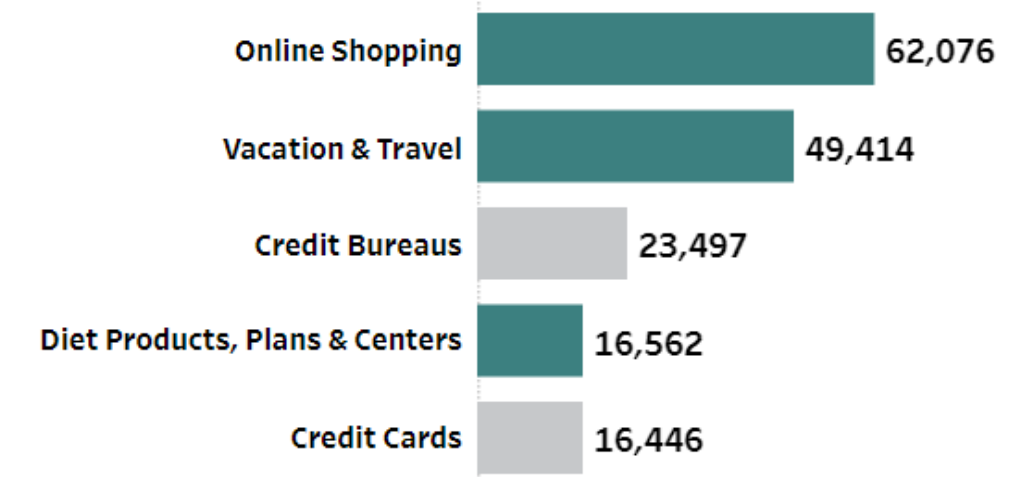


676,167
Overall Reports

\$675.98M
Total Fraud Loss
*44.9% of Fraud reports indicate a loss

\$400
Median Fraud Loss

Top reports were about:



Student Question:

What's the distribution of different types cyber crimes and which ones are most popular, and why?



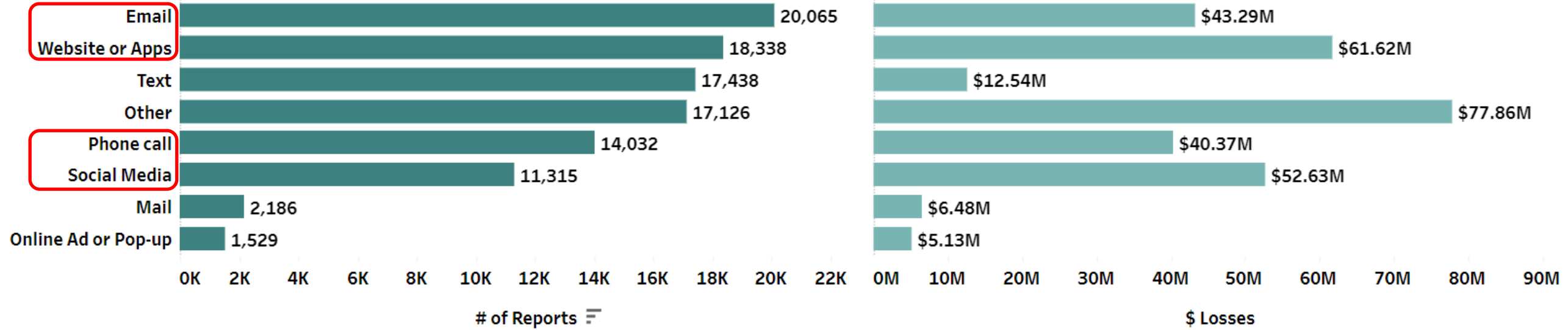
FTC COVID-19 and Stimulus Reports

Fraud Reports

*Data from January 1, 2020 to December 14, 2021

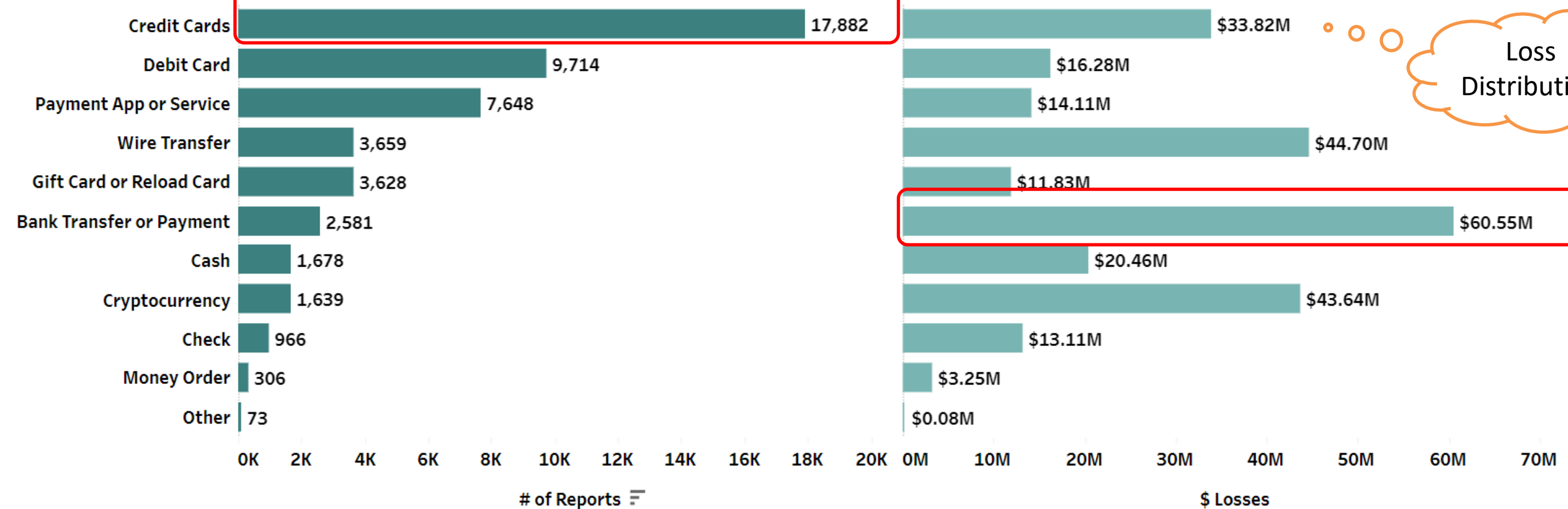
Digital Channels

Contact Method:



Of the total fraud reports, 35.9% indicated a contact method.

Payment Method:



Real-Time Transactions: Irrevocable

Loss Distribution

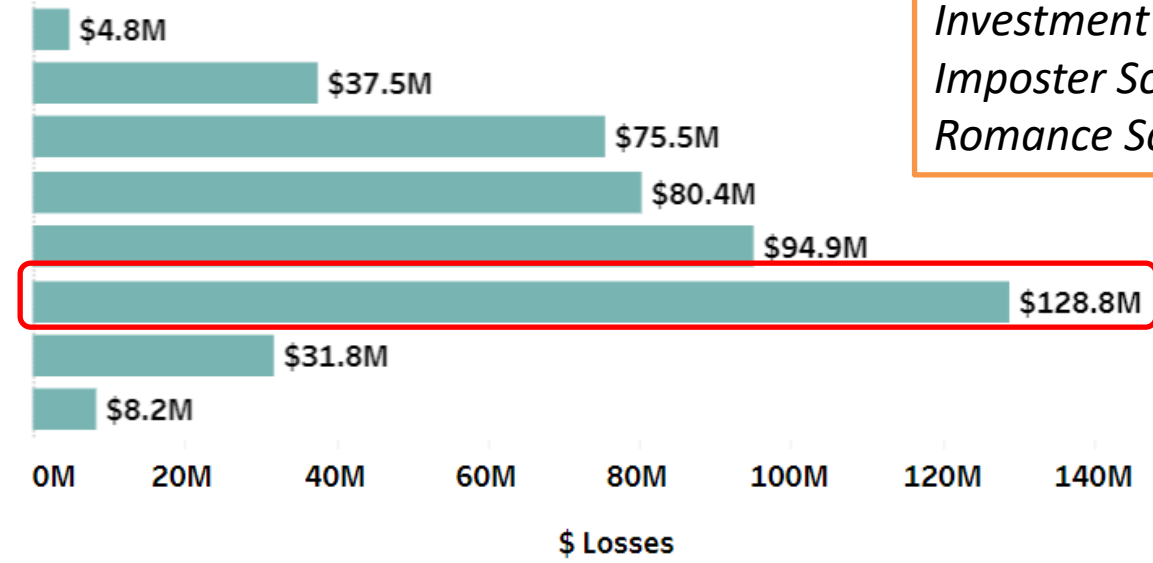
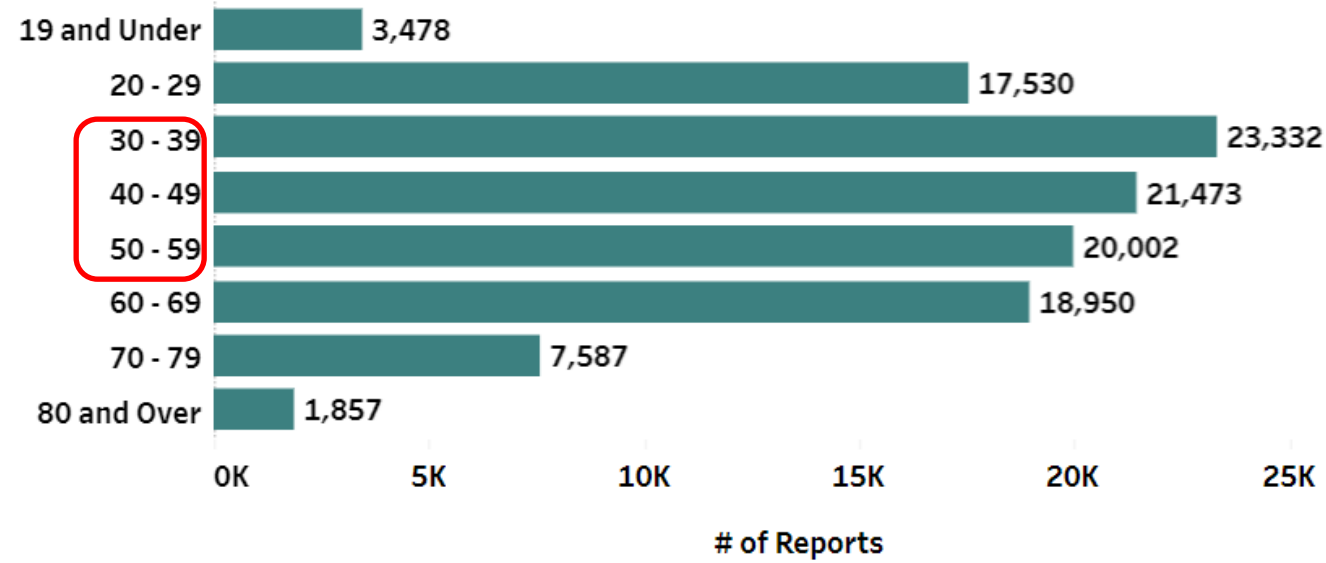


FTC COVID-19 and Stimulus Reports

Fraud Reports

*Data from January 1, 2020 to December 14, 2021

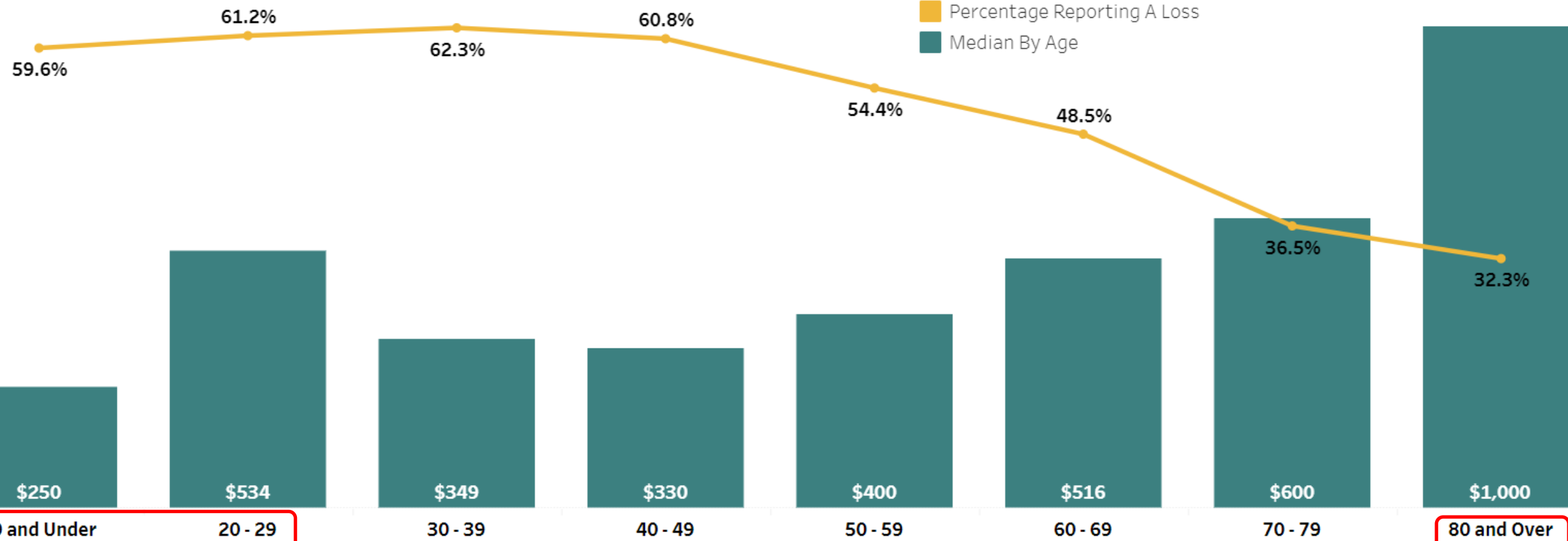
Number of reports and losses by age:



Frequency ↑

Loss ↑

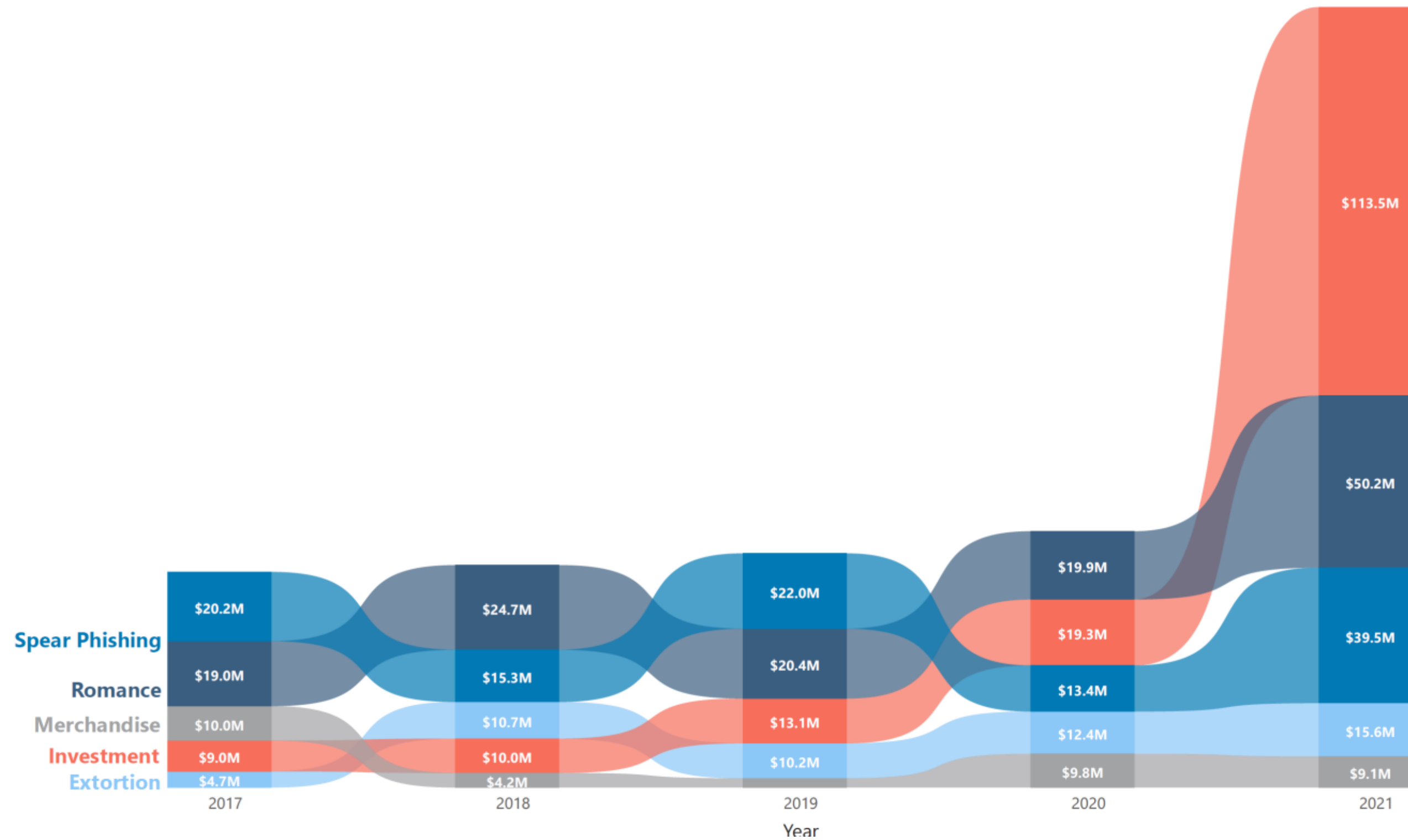
Investment Scam
Imposter Scam
Romance Scam



Virtual Assets Theft
Scareware Attack
Romance Scam
Employment Scam

Elder Abuse

Top 5 - Dollar Loss by Year and Fraud Type



Note: Source from *Canadian Anti-Fraud Centre (2022)*. A screenshot showing Top 5 Dollar Loss by Year and Fraud Type https://publications.gc.ca/collections/collection_2022/grc-rcmp/PS61-46-2021-eng.pdf

Cyber Fraud Victimization In the Context of COVID- 19

Psychological
Physiological
Financial
Social
Technological
...



Cybersecurity

- New Digital Platforms & Technologies
- Working Remotely
- Online Shopping
- Digital Entertainment
- Financial Technology



Well Beings

- Social Isolation
- Life Events: Divorce / Recent Loss
- Travel Restriction
- Separation from Overseas Friends & Families
- Physical Well Beings

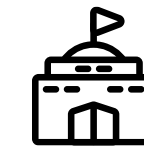


Financial Burden

- Job Loss
- Less Job Opportunities in Service Industry
- Inflation
- Assisting Friends and Families Financially

Possible Vulnerabilities

- Job Scam
- Love Scam
- Emergency Scam
- Remote Access Control Scam
- Government Impersonator Scam
- Download of Malicious Software
- SIM Card Swap / SIM Hijacking
- Text Rerouting / Call Forwarding
- SME Business Executive Scams
- Online Learning Scams
- Phishing / Smishing / Vishing
- Food Bank / Emergency Shelter Scam
- COVID-19 Government Relief Funds Application
- COVID-19 Testing Kits / Cure / Supplement
- COVID-19 Vaccine Certificate Scam
- COVID-19 Contact Tracking Scams
- COVID-19 Donation Scams



For \$16, Companies Can Reroute Your Text Messages To Hackers Without Your Consent



Lee Mercado, Tech Times | 16 March 2021, 11:03 am

MOST POPULAR

1. AstroSwap

Criminological Theories

Understanding COVID-19-themed cyber fraud with traditional criminological theories

01 Anomie Theory

Rapid social changes that occur in an organic society (in this case, the onset of COVID-19) will lead to the state of anomie. *“breakdown of the ability of a society to regulate the natural drives of individuals in the face of rapid social change”*

02 Strain Theory

The emphasis on achieving material gains outweighs the need to follow rules, which leads to individuals using any means necessary, including crime, to achieve such goals under social pressure

03 Rational Choice Theory

Weighing their options

Psychological Vulnerabilities

Classic APP Scams or Social Engineering Techniques

Loneliness

Romance Scams; Sextortion; Companionship Scams; Sugarbaby Scams

Greed

Investment Scams; Cryptocurrencies Scams; Counterfeit Merchandise Scams

Opportunistic

Job Scams; Health or Weight Loss Scams; Fake Lottery Wins; Holiday Scams; Mystery Shoppers Scams; Inheritance Scams; Fake Business Opportunities; Ticket Fraud; Education or Training Fraud; Rental and Housing Scams

Fear of Authority

Taxpayer Scams; Fake Law Enforcement Agencies; Bank Investigator Scams; Fake Collection Agencies; Immigration Scams; Fake Hydro or Utilities; Fake Politician or Influencers Scams; Business Email Compromise or CEO Scams

Curiosity

Psychic Scams; Online Auction Fraud; Free Trial Scams; Wangiri Scams; Gift Card or Shopping Credit Scams; USB Baiting Scams

Distress

Ransomware Scares; Fake Bomb Threat; Help Desk/Tech Support Scams

Urgency or Emergency

Accidents or Emergency Scams; Hostage Scams; Fake Charities

Navigating Cyber Fraud During COVID-19

Why it's important to have an updated typology

- Create Targeted Fraud Strategies
- Improve Procedures and Regulations
- Provide Detection and Investigation Training
- Educate the Public
- Govern Technology Development
- Manage Criminal Activities and Limit Unintended Funding to Organized Crime Rings
- Tailor Victim Services Accordingly
- Reduce Fraud Losses and Increase Fraud Recovery
- Effective Public-Private Partnership





COVID-19 Themed Cyber Fraud Classification

Classification Based on Common COVID-19 Cyber Fraud

- 01 Unauthorized transactions using financial information
- 02 Unauthorized transactions using identity information
- 03 Authorized transactions without fraudulent intent
- 04 Authorized transactions with fraudulent intent



Unauthorized Transactions Using Financial Information

Only the financial information is compromised – not the identity

Cybercriminals in this scenario do have enough financial information to achieve illegal monetary gains through unauthorized transactions

Unauthorized Transactions Using Financial Information



Device Vulnerabilities

- **Compromised Merchants**
 - Online
 - POS Machine
 - ATM
- **Use of Cyber Crimeware:** trojans, viruses, bots (e.g. FriendBot), keyloggers, backdoors, e-skimming, spyware, ransomware, scareware, adware, worms, malicious code and denial-of-service



Domain Spoofing

- **Top-level Domain Spoofing:**
 - who.int vs. who.edu (fake);
- **Typosquatting:**
 - who.int vs. whoo.com (fake);
- **Visual Homograph:**
 - google.com vs. g00g1e.com (fake);
- **Semantic Spoofing:**
 - who.int vs. tedrosadhanom.com (fake);
- **Combination:**
 - who.int vs. w^hoo.edu (fake)



Elder Abuse

- **Social Distancing Concerns:** Leveraging Social Resources for Daily Activities
- “Trusted Others” such as family members, caregivers, neighbours and friends are given access to sensitive financial information
- Max out credit card online / ATM cash out / digital money transfer

Unauthorized Transactions Using Identity Information

An escalation from the previous categories:
A victim's identity information is compromised,
and the cybercriminal gains sufficient information
to engage in cyber fraud

Unauthorized Transactions Using Identity Information



Government Financial Relief Program

- Helping applicants (new immigrants/language barriers/elderly) to file the applications then steal their identities
- Using compromised identity information to file fraudulent financial relief program support
- Impersonating government official to disqualify the benefit receiver then contacting victims for urgent repayment



Contact Tracing Scam

- Contact individuals to inform them that they may have been exposed to COVID-19
- Pay for Testing Kits
- Some contact tracer scammers may even intimidate victims by threatening their immigration status
- Instruct them to download malware by clicking suspicious emails or text messages

Authorized Transactions without Fraudulent Intent

“I did this, but I did not know it was fraud”

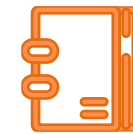
Victims authorizing transactions that are fraudulent in nature but are conducted without victims having fraudulent intent or knowing that they are committing fraud.

Authorized Transactions without Fraudulent Intent



Romance Fraud

- Fake profile
- Building what may feel like a real, loving relationship
- Earning victim's trust
- Ask the victim to help them through a difficult life situation by sending money
- Cheque-cashing scheme: pretend that
- they are living abroad and are unable to cash cheques-
>victims unknowingly commit a crime by cashing a fraudulent cheque
- Variation: Sugar Daddy Scam



Employment Scam

- Advance fee for training
- Buying expensive equipment and supplies to work from home
- Cheque-cashing scheme: wire back the pay cheque difference
- Asked to purchase cryptocurrencies
- Downloading malware for "work purposes"
- Stealing Identification during the hiring process

Authorized Transactions with Fraudulent Intent

The Real Fraudsters

Authorized Transactions with Fraudulent Intent



For Financial Gains

- Filing fraudulent credit card applications
- Misusing credit cards
- Issuing fraudulent cheques
- Abusing online cheque deposit functions
- Busting out credit cards
- Defaulting on loans



Launder Illicit Funds Online

- Digital Entertainment / Online Gambling
- Increased use of virtual assets to move and conceal illicit funds during COVID
- Blackmail attempts, paying for non-existent treatments/equipment, investment scams
- Linked to Organized Crime Rings: Human Trafficking, Drug Trafficking, Terrorist Activities and etc.

Navigating Cyber Fraud During COVID-19

Why it's important to have an updated typology

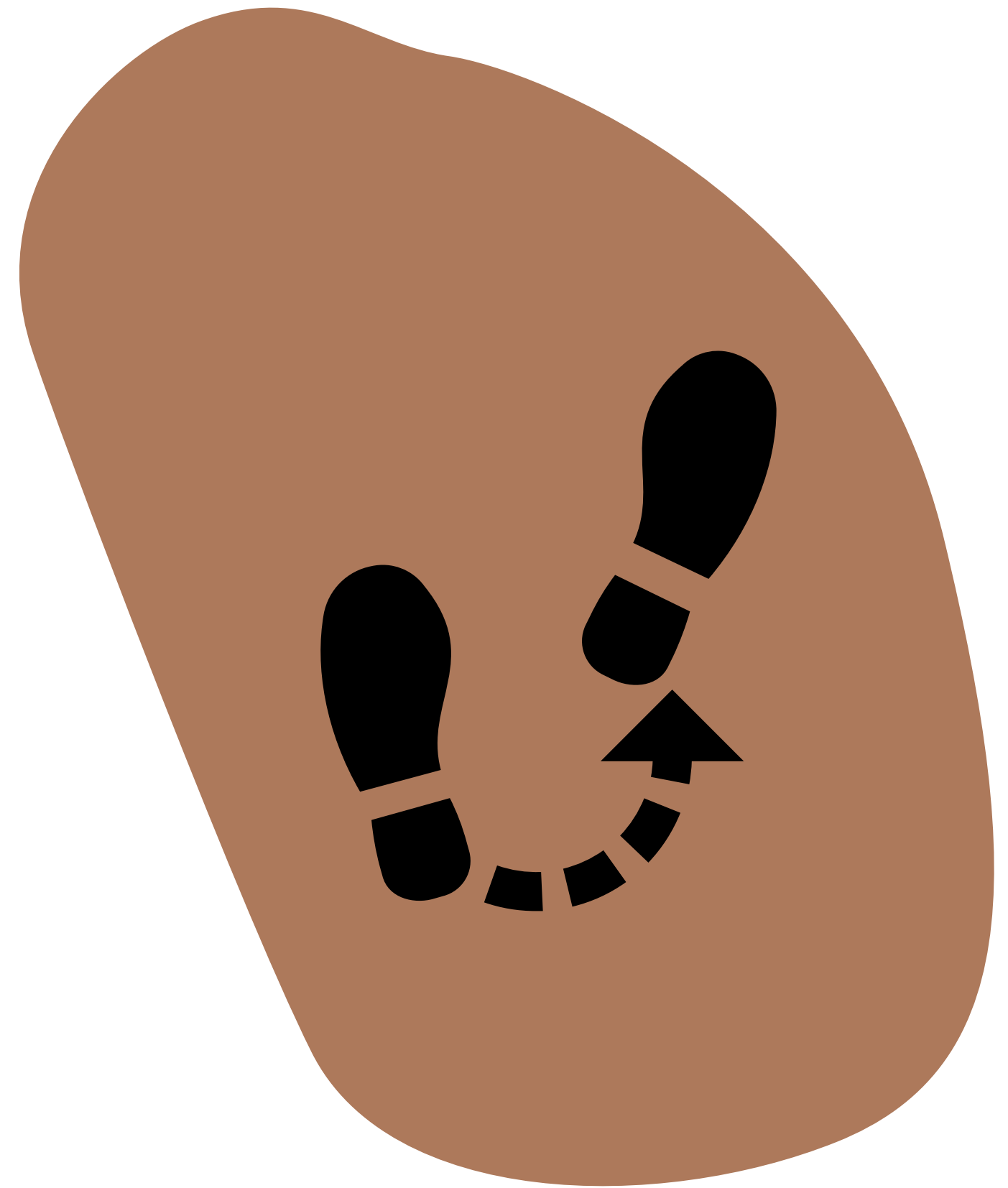
- Create Targeted Fraud Strategies
- Improve Procedures and Regulations
- Provide Detection and Investigation Training
- Educate the Public
- Govern Technology Development
- Manage Criminal Activities and Limit Unintended Funding
- Tailor Victim Services Accordingly
- Reduce Fraud Losses and Increase Fraud Recovery
- Effective Public-Private Partnership





Part Four

Re – Defining Cyber
Financial Crime
Victimization: Financial
Institutions



VICTIMS OF CYBER FINANCIAL CRIME?



Bank card information stolen online



Compromised digital identities



Financial losses through a cybercrime event



WHO ARE THE VICTIMS OF CYBER FINANCIAL CRIME?

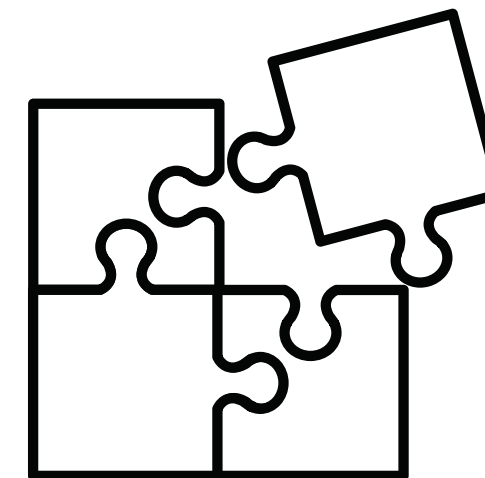
"Victims" means persons who, individually or collectively, have suffered harm, including physical or mental injury, emotional suffering, economic loss or substantial impairment of their fundamental rights

(United Nations Human Rights Office of the High Commissioner, 1985)



ASSUMPTION

Many, therefore, may assume that cyber financial crime victims are those who suffer from financial losses through a cybercrime event



Is this perception true, however? More specifically, for our purposes, is this perception true in North America?



POINT 1: CONTESTED DEFINITION

While this definition is certainly valid in some cases, it is not always applicable and may be contingent on circumstances or contexts.

Financial institutions in North America play a significant role in defining and classifying cyber financial crime victimization.



POINT 3: NON-GOVERNMENTAL REGULATION

While North American financial institutions are not public law enforcement agencies, when it comes to cyber financial crime, major banks work together in order to regulate and manage cyber financial crime.



POINT 2: SOCIAL CONSTRUCTION OF VICTIM IDENTITIES BY INSTITUTIONS

Social construction of North American victim identities in the digital era can be shaped by non-governmental institutions.

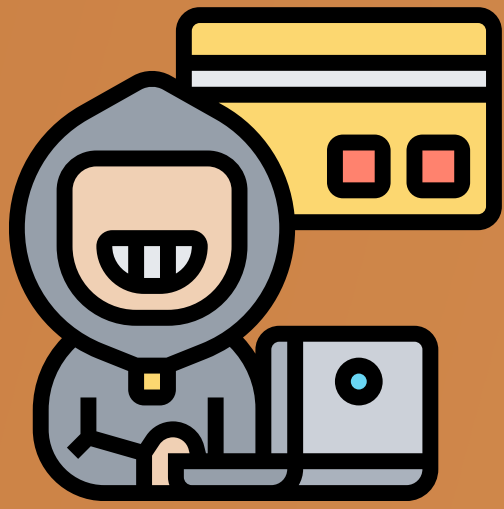
Power to detect, investigate, interpret, determine, adjudicate, and even punish cyber financial crime.



The role of non-governmental institutions, such as financial institutions, in producing, using, disseminating, and contesting authoritative concepts and knowledge related to cyber financial crime

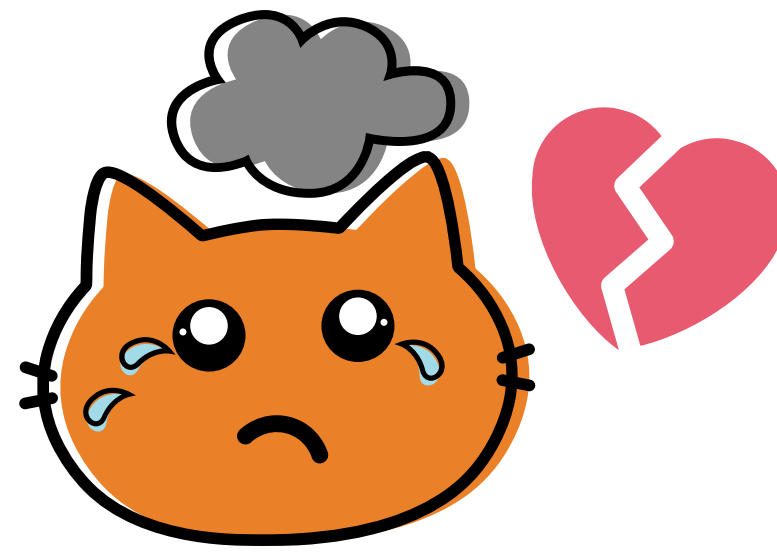
Student Question:

Real stories of cyber criminals and cyber security defenders. Case studies?



CASE I

- Job scam victim
- Fake paycheck
- Deposited and attempted to withdraw



CASE II

- Love scam victim
- Shared account
- Deposited stolen money (proceeds of crime)



CASE III

- Phishing link victim
- Stolen credentials
- Applied for fraudulent credit cards online

CO-CONSTRUCTING

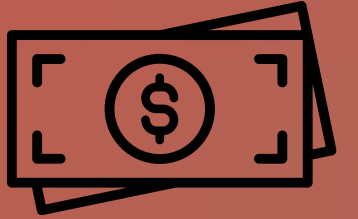
When North American financial institutions produce victim identities, they are co-constructing the knowledge and political order together with:

- the perpetrators
- the victims
- the governments
- the law enforcement agencies
- the media
- other financial institutions
- and other public actors including regulatory bodies

The social construction of cyber financial crime victim identities in the digital era can be shaped by North American financial institutions' governance guidelines, bank card holder agreement and policies, and operational procedure.



The investigation and adjudication decisions are not static; they are fluid, and embedded within sociotechnical interactions and cognitive assumptions.



DISCUSSIONS

- Fluid definitions and interpretations of cyber financial crime victimization
- North American financial institutions are shaping and reproducing the concept of cyber financial crime victimization on an ongoing basis through daily customer interactions, which continually legitimizes the process.
- Co-existing identities as both victims and perpetrators
- Interestingly, the perpetrator identity can quickly shift to the victim identity if the customer threatens legal action or media exposure.
- Claims can be legitimized based on an institution's unique customer knowledge
- Victimization due to cyber financial crime varies on a case by case basis, and levels of innocence and guilt can also vary.



Student Question:

Why bank systems (transactions, platform services) are so slow? Is there any particular reasons for that?

Human Actors	Non-Human Actors
Cybersecurity Companies	Digital Banking Applications or Interfaces
Financial Institutions	Telecommunication Infrastructure
Telecommunication Service Provider	Malicious Codes
Users / Consumers with Psychological Vulnerabilities	Anti-Virus Software
Cybercriminals / Organized Crime Rings	OTP / Two Step Verification
Governmental Agencies	Phishing Emails / Calls / Mails / Text Messages
News Media	Digital Devices including Servers
Online Merchants / Vendors / Service Providers	Websites
Financial Technology Companies	Network Technologies
Regulators	Consumer Credentials
Payment Service Providers	Digital Payment Methods
Policy Makers	Quantum Computing
Cybercrime Victim Services	Blockchains
Social Media Companies	Government Assistance Funds
Application / Software Development Companies	Bank Accounts
Disadvantaged Social Groups	Payment Transfer Systems
Relationship Abuser	Online Service Platform
Human Trafficker	Email Accounts
Gift Card Retailors / Money or Remittance Services	Social Media Advertisement

THANK YOU

Presented by
Katelyn Wan Fei Ma

Let's Connect!
@KatelynWanFeiMa



Ph.D Candidate @ Graduate Program
in Science and Technology Studies
York University



Lecturer, Department of Criminology,
Faculty of Human and Social
Sciences, Wilfrid Laurier University



America's Most Convenient Bank® American Fraud Operations

Manager of Strategic Initiatives, North