

Who is the Customer YOU Know?

# Disclaimer for Information Security Presentations

Neither Bank of America nor its affiliates provide information security or information technology (IT) consulting services. This material is provided "as is," with no guarantee of completeness, accuracy, timeliness or of the results obtained from the use of this material, and without warranty of any kind, express or implied, including, but not limited to warranties of performance, quality and fitness for a particular purpose. This material should be regarded as general information on information security and IT considerations and is not intended to provide specific information security or IT advice nor is it any substitute for your own independent investigations. If you have questions regarding your particular IT system or information security concerns, please contact your IT or information security advisor. Neither Bank of America nor its affiliates shall be liable for any content in this presentation or your use of it.

# Agenda

- Setting the stage: Addressing fraud trends together
  - Providers
  - Customers
- Viewpoint
  - Financial
  - Corporate
- KYC: Recommendations for improvement

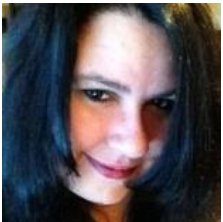


# Presenters



Guy Pearson leads the Adversarial Threat Intelligence team at Bank of America. This includes identifying the 'who and how' for threats to associates, clients and the industry.

eMail: [Guy.V.Pearson@bofa.com](mailto:Guy.V.Pearson@bofa.com)



Mary Anne Conner is a SVP/Senior Technology Manager within Bank of America who is responsible for ensuring the network effectively and securely manages hundreds of millions of incoming and outgoing telco communications.

eMail: [mary\\_anne.conner@bofa.com](mailto:mary_anne.conner@bofa.com)



# Setting the stage

- Increasing threats passing through telecoms:
  - 20% of fraud is phone related
  - Not just targeting consumers:
    - FBI: Spoofing, vishing, & smishing are key parts of business email compromise
    - FBI & CISA: Scattered Spider exploits SIM swaps, smishing and phishing to infiltrate businesses
  - Help Net Security survey:
    - 61% of enterprises did not invest in SMS/voice defense
    - 51% believe telecoms protect them

## Phone-based Phishing Growing Unchecked



Anti-Phishing Working Group 1Q24

[Anti-Phishing Working Group 1Q24 report](#)

[Spoofing and Phishing — FBI](#)

[FBI, CISA warn of Scattered Spider hackers targeting commercial facilities, adopt social engineering techniques - Industrial Cyber](#)

[Vishing, smishing, and phishing attacks skyrocket 1,265% post-ChatGPT - Help Net Security](#)




# Viewpoint from a Financial Client

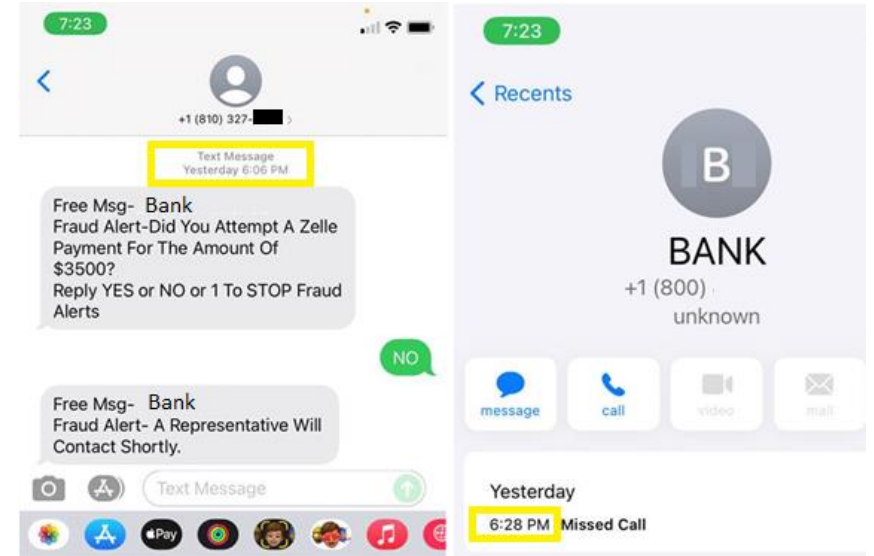
Criminals leverage branding to instill a false sense of confidence in victims, and manipulating our clients into falling for scams

 Criminals improve targeting with compromised info

Results:

- Impersonations are more impactful
- Text & Voice impersonations more effective

 Est. 1 in 5 brand recognizable line calls were spoofed  
Est. 6% of incoming calls have high risk signals



## Financial clients need consistent partnership

Detect and defend against unlawful impersonations:

- Identify & engage exploited sources
- Delivered impersonation texts
- Spoofed call campaigns

Impersonated Institute	Count of Calls	Impersonated Institute	Count of Calls	Impersonated Institute	Count of Calls
FI 1	22,461	FI 7	41	FI 13	22
FI 2	6,238	FI 8	30	FI 14	20
FI 3	2,037	FI 9	29	FI 15	19
FI 4	545	FI 10	27	FI 16	16
FI 5	83	FI 11	52	Carrier 1	151
FI 6	75	FI 12	24		

Example of an impersonated text/call & one call spoof campaign <sup>6</sup>



# Viewpoint from a Corporate Client

## Criminals seek unlawful access to your network



- Criminals use registered intellectual property in text and voice to deceive employees
- Groups like Scattered Spider do their research

### Results:

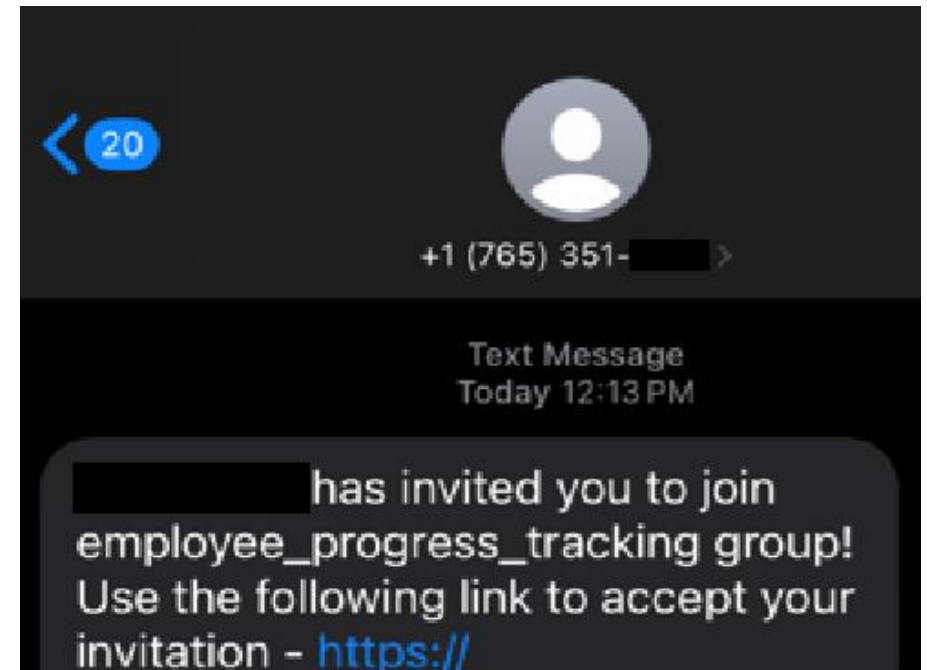
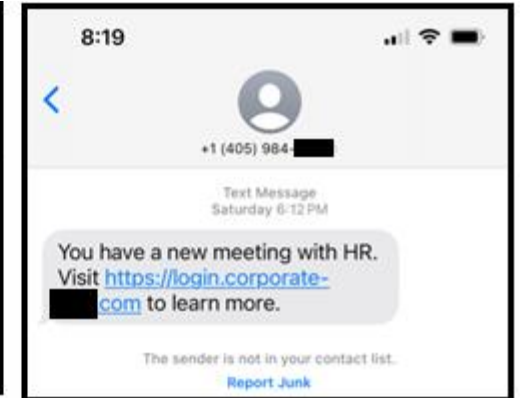
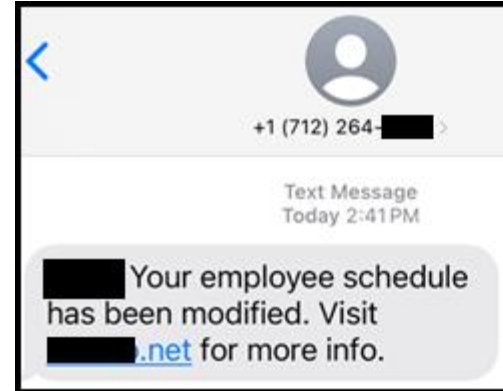
- Effective targeting of employees



- Texts or calls received on both corporate and personal devices
- Branding can be found in source, text body or URL

### Corporate clients need consistent partnership

Detect and defend against social engineering passing through text and voice channels



# Know Your Customer

More enhanced thought process for KYC, encompassing Enterprise Customers more than “just” the mobility customer

- Identification (and population) of customers and their data
- Customer Analysis/Risk Assessment (IP validation, STIR/SHAKN)
- Advanced risk Assessment(PASSports)





# Identification of customers and their data

Identifying, communicating and understanding Enterprise customers will optimize data and security

- Number Identification
- IP Peering, VLAN Tagging
- Identification, communication, and strategic planning to resolve internal company technical limitations



# Customer Analysis/Risk Assessment

Identifying, communicating and understanding Enterprise customers will optimize data and security

- STIR/SHAKN
- IP Peering/VLAN Validation
- Legacy systems
  - API's for systematic validation
- Cross organizational communication
- Cross vendor communication
- Blacklisting/Fraud Detection based on risk assessment



# Advanced risk Assessment(PASSporT)

Leaving the customer out of an end to end solution

- End at the Carrier
- PASSporT
- RCD



# Summary: Create Roadmap Together

## Process concerns:

- Communication vendors processing and actioning LOAs for Enterprises with no due diligence (validation of individuals, emails, etc.)
- Carriers allowing action of LOAs without Enterprise validation
  - **Creates foundation for bad actors to act**

## Privacy concerns:

- FCC stated: 47 USC 222 Section D2 enables carriers to “*use, disclose or share sensitive information*” to protect consumers from “*fraudulent, abusive, or unlawful use*” of their services
  - **Do we need further clarification to partner & fight unlawful traffic?**

## Security concerns:

- Delegate PASSport, signed certs extended to the Enterprise.

 **Voice is Data – why are we treating it differently?**