

ALTA **in**SIGHTS

REAL TIME | ON-DEMAND



The State of Wire Fraud:
2022 Trends & Industry Forecast

Today's
ALTA Insights
Featured
Sponsor



The State of Wire Fraud:

2022 Trends & Industry Forecast



You know wire fraud is a problem. **But how bad is it?**

Escalating losses impact reinsurers, underwriters and agents.

INTRODUCTION

Why is wire fraud a big problem?

Typically large sums of money involved.

Increasing speed of transactions.

Accessible to anyone with a bank account.

Targets any sector with weak infrastructure and lax cybersecurity.

\$10.3B

in **cyber crime reported** in 2022¹

4x

increase in **BEC losses**
from 2017 to 2022²

83%

of CertifID customers had transactions
with suspected fraud in 2022³

¹ [FBI Internet Crime Report 2022](#)

² [FBI 2022 Congressional Report on BEC and Real Estate Wire Fraud](#)

³ [CertifID, State of Wire Fraud, 2022](#)



INTRODUCTION

Why is wire fraud such a problem in real estate?

Open source information, MLS syndication and multiple transactional parties make real estate a top target.



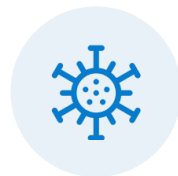
Real estate transactions are **complex**



They involve a **lot of money** and **a lot of people** (8 different parties on average)



Much of the information scammers need to trick you is **publicly available** on the internet



The COVID-19 pandemic led to a rapid growth in digital closings **without creating a safety net**



A series of thin, light blue wavy lines that curve from the top left towards the bottom left, creating a sense of motion or a stylized background element.

State of Wire Fraud

FBI: 2022 IC3 Report

Cybercrime on the rise

39
seconds

In 2022, a cyber crime was reported once every 39 seconds.



\$10.3B
losses

Total cyber crime losses in 2022 reached \$10.3B.



Reported losses into the FBI reached another all-time high in 2022.



Top cyber crime types by loss



\$3.3B

Investment



\$2.7B

BEC



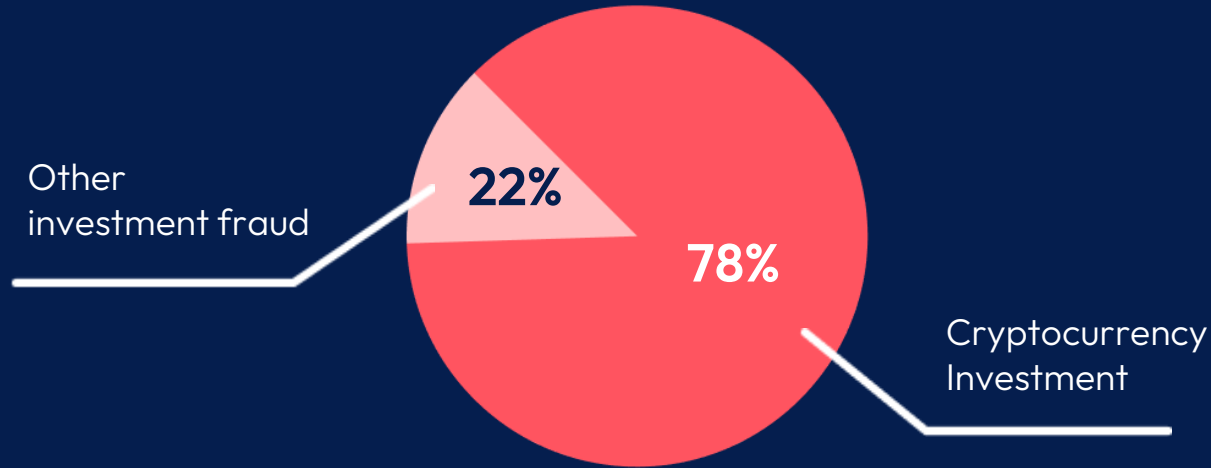
\$0.8B

Tech Support

Business Email Compromise (BEC) at \$2.7B represented 26% of all reported cyber crime losses.



Investment losses



Investment fraud (led by pig butchering scams) became the largest source of losses in 2022, of which 78% were cryptocurrency scams.



Business email compromise (BEC)

How BEC works:

- 1 Open source intelligence
- 2 Social engineering
- 3 Account takeover
- 4 Attack email
- 5 Funds transfer

BEC losses increased by 4x over the past five years.



\$676M

12,005 victims

in 2017



\$2.7B

21,832 victims

in 2022



Demographics are shaping the scam vectors



Investment

\$3.3B in 2022 loss

Majority aged 30-49

Hacked social media
Cryptocurrency
Celebrity impersonation
Real estate
Employment



BEC

\$2.7B in 2022 loss

All ages

Hacked email
Social engineering
Spoofed phone calls
Fraudulent accounts



Call Center Fraud

\$1B in 2022 loss

Majority aged 60+

Customer support
Tech support
Government impersonation



Business email compromise (BEC)

BEC targets businesses and individuals performing transfers of funds.

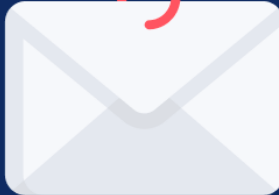
Cryptocurrency has enabled accelerated funds movement.

Compromise has evolved into spoofed phone, video, websites, etc.

BEC losses increased by 4x over the past five years.

2017

\$676M
12,005 victims

2022

\$2.7B
21,832 victims

Top cyber crime types by victims



300K

Phishing



59K

Personal data breach



52K

Non-payment/ Non-delivery

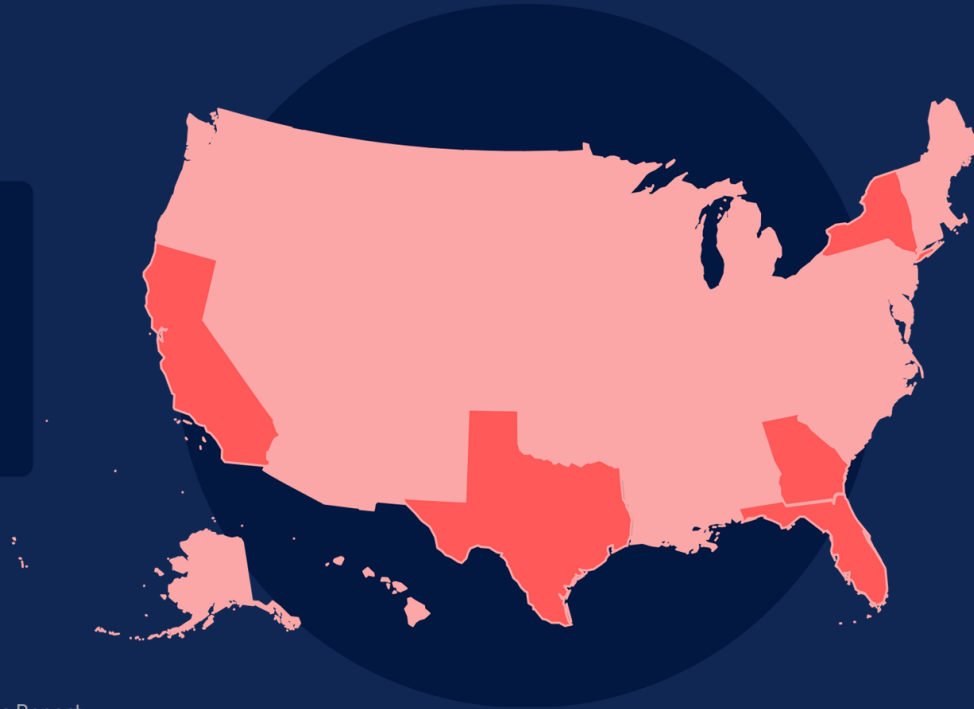
Phishing (inclusive of vishing, smishing, and pharming) affected the most victims of all crime types.



Who is at risk?

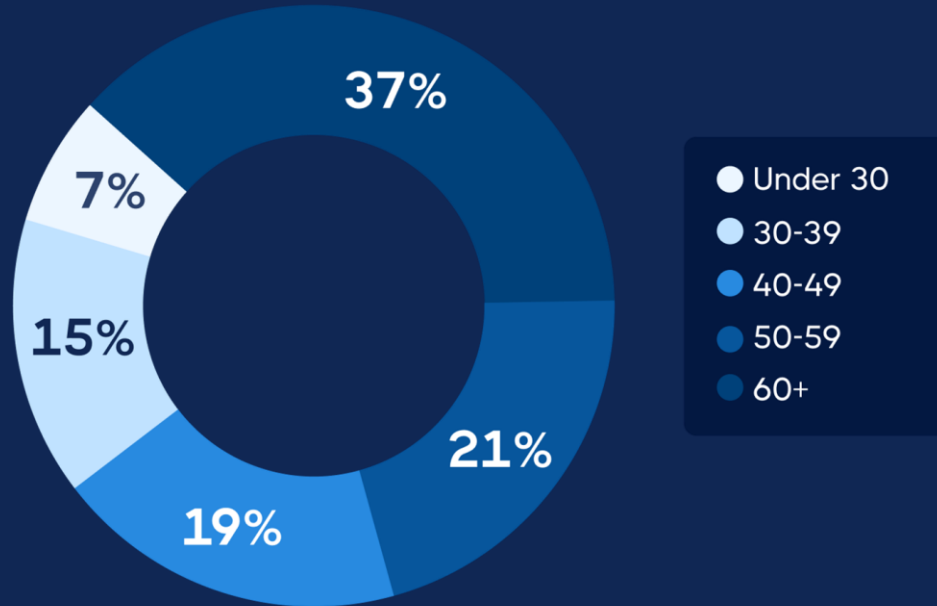
All U.S. states reported losses, with the top 5 states representing 46% of all victim losses.

- California
- Florida
- New York
- Texas
- Georgia



Victims span all age groups.

Victims age 30-49 are the most targeted for investment scams.
Victims over 60 represent the majority of call center fraud losses.



Demographics are shaping the scam vectors



Investment

\$3.3B in 2022 loss

Majority aged 30-49

Hacked social media
Cryptocurrency
Celebrity impersonation
Real estate
Employment



BEC

\$2.7B in 2022 loss

Hacked email
Social engineering
Spoofed phone calls
Fraudulent accounts



Call Center Fraud

\$1B in 2022 loss

Majority aged 60+

Customer support
Tech support
Government
impersonation



For a summary of all the results:

<https://www.certifid.com/infographic/2022-cybercrime-trends>

State of Wire Fraud

CertifID: Fraud Recovery Services

Fraud cases climbed at an unprecedented rate.

The CertifID Fraud Recovery Services (FRS) team received an unprecedented number of reports of wire fraud.



145%

increase in cases
reported, year over year



1 in 4

cases submitted
could be worked



\$158k

average loss reported
per case

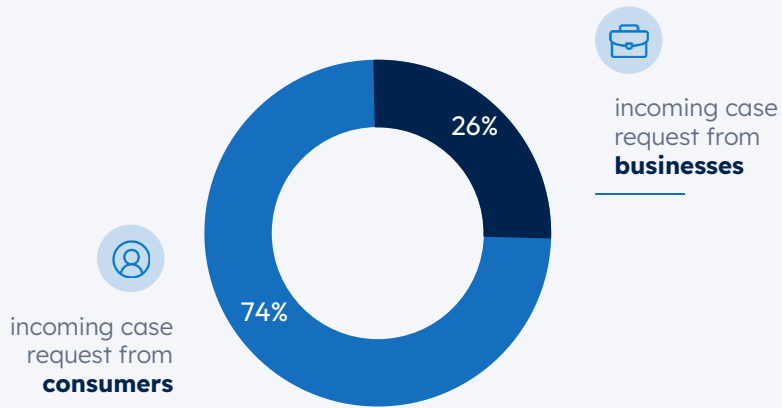


6.5 days

average time from
incident to recovery

Businesses suffered losses 3x as large as those of consumers.

Consumers are hit more often, but businesses are hit for larger sums.



\$294,573

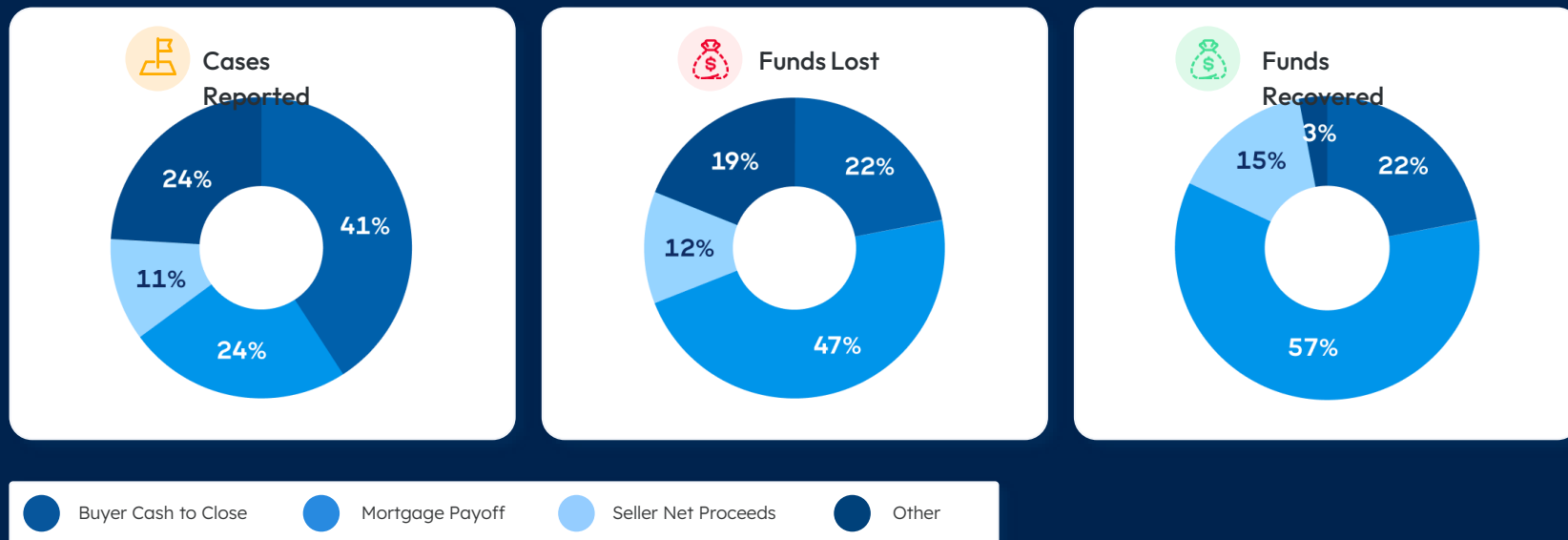
Average wire fraud loss for business cases

\$106,557

Average wire fraud loss for consumer cases

Every stage of the real estate transaction is vulnerable.

The buyer's cash to close, the seller's net proceeds and mortgage payoffs are all at risk.



State of Wire Fraud

CertifID: Protection Software

What tools can help prevent fraud?

Of the over 340k in transactions processed by CertifID in 2022, \$1.4B worth were flagged as suspected fraud.

340k

wire transactions **verified**
by CertifID

\$1.4B

in suspected fraud identified
across **all transactions**
processed

83%

of customers who
had transactions with
suspected fraud



2022 TRENDS

Scammers especially target mortgage payoffs.

In 2022, CertifID was able to verify and protect against payoff fraud in over 95% of all requests submitted.



32k

payoff transactions processed



\$7.5B

in payoffs protected



\$5.5M

in fraud caught and prevented





State of Wire Fraud

Latest Trends and Forecast

State of Wire Fraud

Wire Fraud Trends: Buyer Closing Funds

State of Wire Fraud

Wire Fraud Trends: Seller Impersonation

Seller Impersonation Scams – Case Study 1

Parcel Identification

Parcel Number: 41-13-22-431- [REDACTED]

Government Unit: 51 - CITY OF GRAND RAPIDS

Owner Name One: YOST [REDACTED]

Owner Name Two:

Property Address: [REDACTED] RAVINE DR NW

Property Classification: 402 - RESIDENTIAL-VACANT

School District Number & Name: 41010 - GRAND RAPIDS CITY SCH DIST



Seller Impersonation Scams – Case Study 1

REDFIN

City, Address, School, Agent, ZIP

1-844-759-7732

Buy

Rent

Sell

Redfin Premier

Mortgage

Real Est

Search

Overview

Property Details

Sale & Tax History

Public Facts


Schools

Favorite

Edit Facts

Share

OFF MARKET



Street View

634 Ravine Dr Nw, Grand Rapids, MI 49504

Redfin Estimate

Beds

Baths

0.48 Acre (Lot)

Off Market

Is this your home?

Track this home's value and nearby sales activity

I own 634 Ravine Dr Nw

\$45,000 List Price

Sale and tax history for 634 Ravine Dr Nw

Sale History

Tax History

Today

Mar 21, 2023

Date

Pending

MIRealSource-MIMLS #70303812

Price

Mar 12, 2023

Date

Listed (Active)

MIRealSource-MIMLS #70303812

Price

Mar, 2023

Mar 21, 2023

Date

Pending

REALCOMP #65023007186

Price

Mar 12, 2023

Date

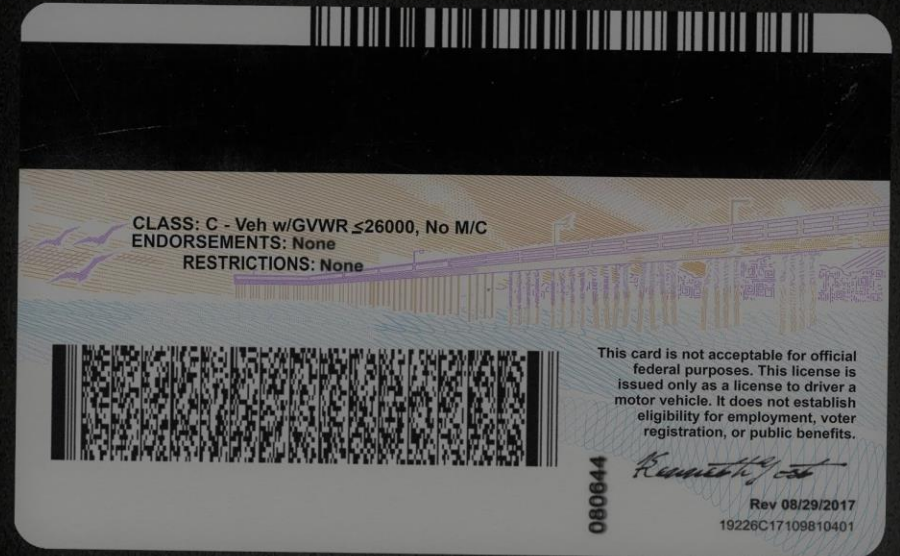
Listed (Active)

REALCOMP #65023007186

Price



Seller Impersonation Scams – Case Study 1




Seller impersonation will continue to climb.

Fraudsters profile vacant or non-owner occupied property and impersonate the owner in order to steal the proceeds.

Download this recently issued US Secret Service advisory so you know what to look for:

[US Secret Service: Vacant Lot Advisory](#)





United States
Secret Service
Cybercrime
Investigations

Real Estate Scams
Vacant Properties

The U.S. Secret Service has observed a sharp increase in reports of real estate fraud associated with vacant and unencumbered property. Criminals are posing as real property owners and through a series of impersonations are negotiating the sale of properties which are vacant or lien free. Criminals are using similar techniques that continue to be deployed in real estate specific Business Email Compromise (BEC) schemes, to include open-source research. Visit the Secret Service website for [guides on BECs and other cyber-enabled financial crimes](#).

the scheme

- ❖ The criminal searches public records to identify real estate that is free of mortgage or other liens and the identity of the property owner. These often include vacant lots or rental properties.
- ❖ The criminal poses as the property owner and contacts a real estate agent to list the targeted property for sale, and requests it being listed below current market value to generate immediate interest.
- ❖ The criminal, posing as the property owner, demonstrates preference for a cash buyer, and quickly accepts an offer.
- ❖ The criminal, posing as the property owner, refuses to sign closing documents in person, and requests a remote notary signing.
- ❖ The criminal (or co-conspirator) also impersonates the notary and provides falsified documents to title company or closing attorney.
- ❖ Title company or closing attorney unwittingly transfers the closing proceeds to criminal.
- ❖ All communication is electronic, not in person.


The fraud is often discovered when recording the transfer of documents with the relevant county. This scheme has particularly affected elderly and foreign real property owners, but it is not limited to these groups, because there are no means to automatically notify the legitimate owners. Therefore, the burden of verification is on the real estate and title companies.

how to prevent

- ✓ Independently search for the identity and a recent picture of the property seller.
- ✓ Request an in-person or virtual meeting and to see their government issued identification.
- ✓ Be on alert when a seller accepts an offer below market value in exchange for receiving the payment in cash and/or closing quickly.
- ✓ Never allow a seller to arrange their own notary closing.
- ✓ Use trusted title companies and attorneys for the exchange of closing documents and funds.

Version 1.1

www.secretservice.gov/contact/field-offices



State of Wire Fraud

Wire Fraud Trends: Weaponizing Technology

The cyber risk digital divide.

Emerging technologies and expanded personal digital footprints create a growing divide between businesses that protect their customers and those that don't.



Vulnerable businesses

- Reliant on belief in trusted communications.
- Focus on manual detection of suspicious behavior.
- Believe they're too small to be a target.

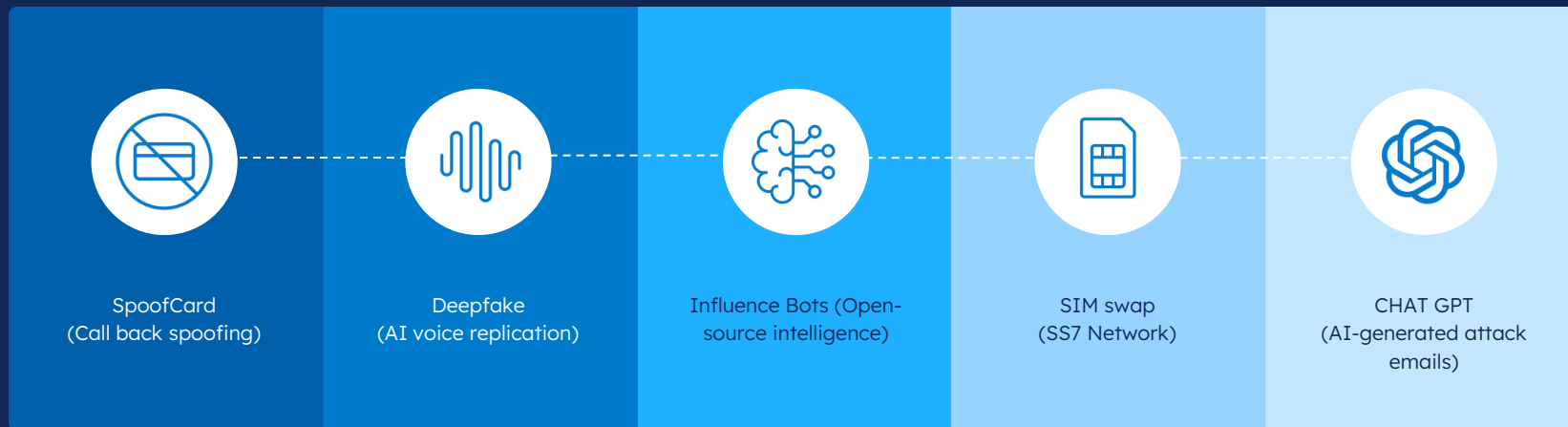


Protected businesses

- Verify identities before sharing sensitive information.
- Leverage technology to inspect every case thoroughly and efficiently.
- Know that everyone is a target.

New tech = new social engineering opportunities.

Scammers have access to more resources than ever before to perfect the attacks that lead to wire fraud.





“We’ve made huge strides in awareness on wire fraud. Now, in addition to providing resources and education, we’ve codified the use of wire verification services as an industry best practice for 2023.”

Diane Tomb

CEO of ALTA (American Land Title Association)



State of Wire Fraud

Wire Fraud Trends: Mortgage Payoffs

Payoff Fraud Caught: \$1.6M

- Title company received a PDF with payoff instructions via lender email
- Submitted for verification by PayoffProtect and flagged as high risk
- CertifID spoke with the lender and servicer and confirmed fraud within hours
- Fraudster then sent a 2nd set of false instructions, also caught by the team before accurate instructions were finally obtained

The preferred method for expedited payoff remittance is by wire transfer.
Wire to:
Bank: Chase Bank, Trenton, NJ, ABA Nbr. [REDACTED]
Beneficiary Name: [REDACTED]
Beneficiary Address: [REDACTED]
BNF Account Number: [REDACTED]
•originator to BNF Info: Attention Payoff Department
Include sender's contact name and phone number



State of Wire Fraud

Wire Fraud Trends: Insurance Protection

A layered approach.

Education and engagement

Technology to lower risk

Insurance coverage to protect from loss

Incident response plan to mitigate impact



Education



Protection Software



Insurance



Recovery Services

State of Wire Fraud

Wire Fraud Trends: Best Practice 4.0

The background of the slide is a solid dark blue. On the left side, there are several thin, light blue wavy lines that curve from the top left towards the center, creating a sense of movement or depth.

Thank you!



Matt McBride

VP of Compliance & Risk Management
Shaddock National Holdings
mattm@shaddocknational.com



Tom Cronkright

Co-Founder & Executive Chairman
CertifID
tcronkright@certid.com

