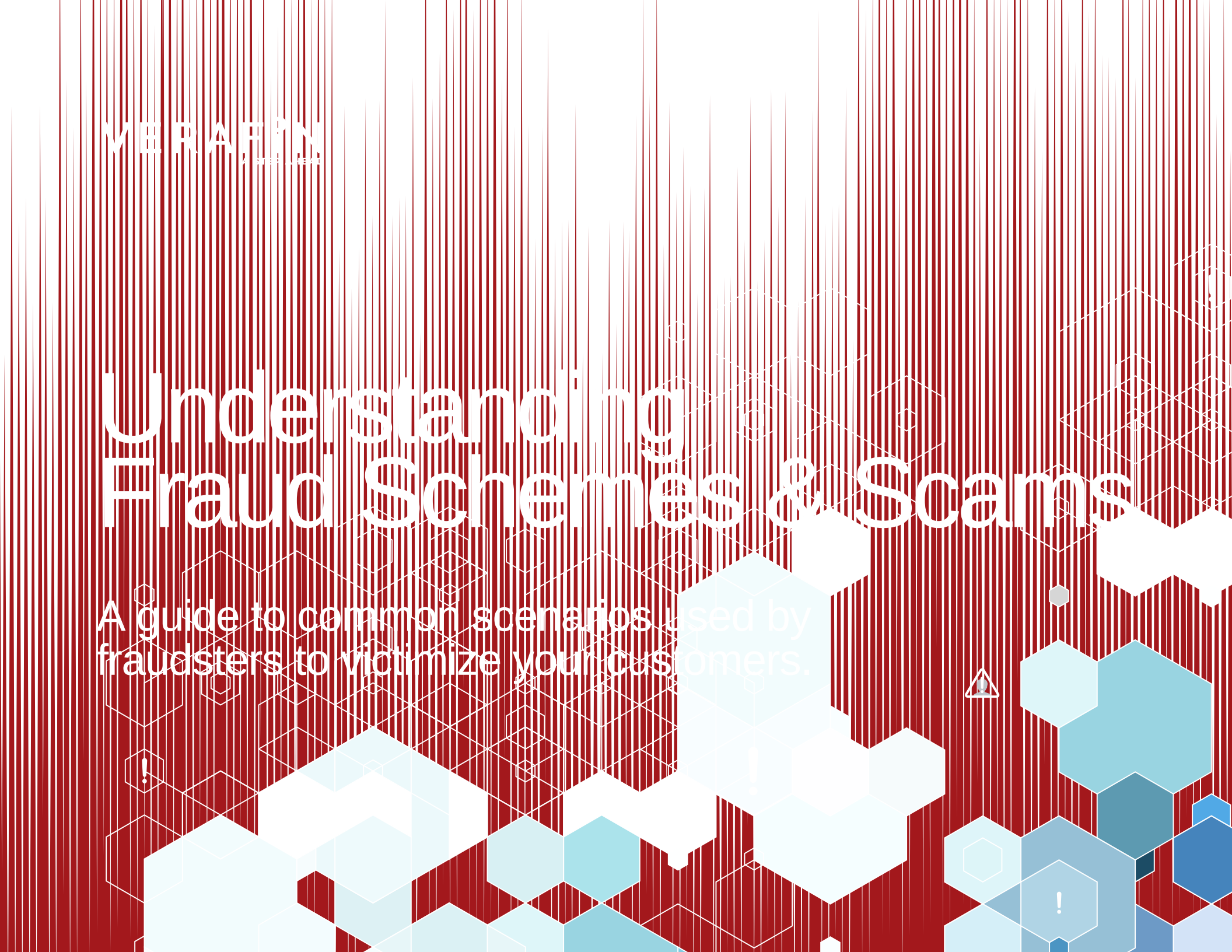
VERAFIN

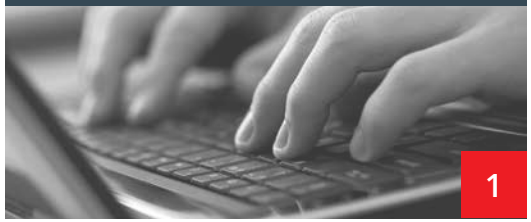
Understanding Fraud Schemes & Scams

A guide to common scenarios used by fraudsters to victimize your customers.



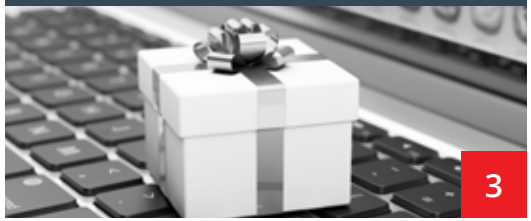
Sections

BUSINESS EMAIL COMPROMISE

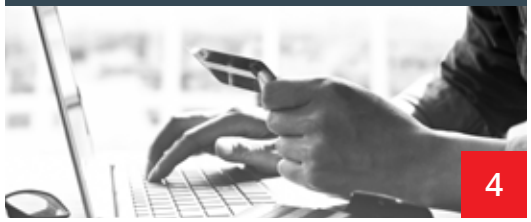


EMPLOYMENT SCAMS

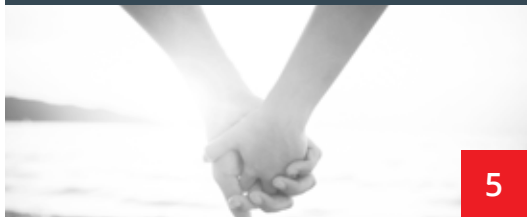
LOTTERY SCAMS



ONLINE LOAN & PAYDAY SCAMS



ROMANCE SCAMS



WHO'S MOST AT RISK?

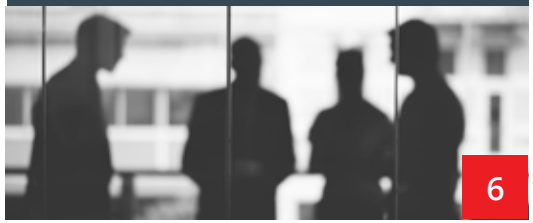


TABLE OF CONTENTS

Introduction

Fraud is constantly evolving — it is the one truth within the industry — and increasingly fraudsters are targeting your customers to commit it.

From secure card technology like EMV/CHIP to improved authentication methods such as biometric and two-factor authentication, financial institutions are creating better security to protect customers and their data.

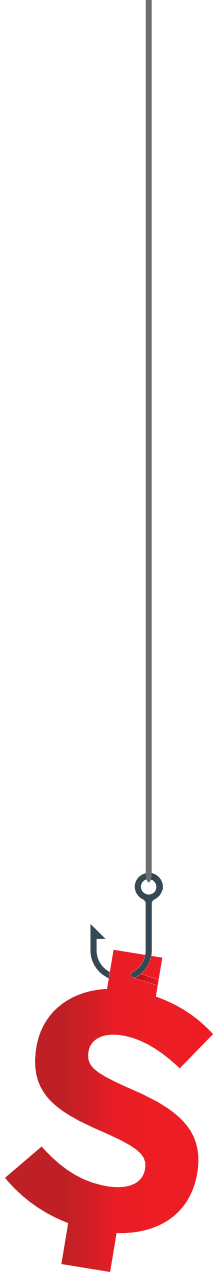
Fraud Scams

These improvements are directing fraudsters to increasingly target the weakest link in these systems — **your customers**. While fraud scams are not necessarily new, they continue to evolve as fraudsters make the adjustments needed to avoid the improved controls across the financial industry.

Fraudsters are taking advantage of two major trends to facilitate these attacks:

1. **Demographic shifts:** an aging population and changing regional economic prosperity are creating a large pool of potential victims for fraudsters to target.
2. **Online and digital channels:** new products and services offered by financial institutions such as mobile deposit, and online or mobile banking.

We have designed this guide to help those combating fraud within financial institutions learn about these scams. The following information was gathered from industry sources, as well as countless interviews with passionate financial crime investigators from the over 1500 financial institutions we work with across North America.



SECTION 1

Business Email Compromise (BEC)

What is it?

***Business Email Compromise** targets a business or commercial client to initiate a large funds transfer to an account under the fraudster's control.*

Who are the victims?

Individuals within a business or corporation who can initiate a funds transfer, such as CEOs, CFOs, Accountants, Bookkeepers, or Accounts Payable.

How does it work?

Fraudsters begin by conducting research on individuals, often in high-level corporate positions. They use online sources of information, including LinkedIn profiles and bios included on a company's web site.

Once individuals are identified, fraudsters will use targeted techniques such as spear phishing to gain access to corporate systems. The fraudster will monitor and research how financial transactions are conducted before initiating their attack.

Fraudsters will generally initiate an urgent and time-sensitive request for a funds transfer. This request will appear to come from a senior officer of the company.

The email, which appears to be from a senior officer, instructs the receiver to urgently transfer significant funds to an account within the fraudster's control (either directly or through a money mule). Fraudsters are adapting to new corporate controls by requesting smaller domestic transfers.

Fraudsters often initiate their transfer request when the senior officer is profiled, such as when on vacation or traveling, to reduce the ability of the person receiving the fraudulent email to verify the request.

What are the indicators?

- **Large wire or funds transfer to a recipient** the company has never dealt with. previously
- **Transfers initiated near the end-of-day** (or cut-off windows) and/or before weekends or holidays.
- **Receiving account does not have a history of receiving large funds transfers.**
- **Receiving account is a personal account** and the company typically only sends wires to other businesses.

How to mitigate the risk?

- **Targeted training** of key financial officers for your business and corporate clients.
- **Callback procedures** for certain fund transfer types.
- **Training for internal staff** (Account Managers, BSA, Fraud, Wire Room, etc.) to identify BEC.
- **Detection systems** that profile both sending and receiving accounts of a funds transfer to ensure the activity is typical for both parties.

Resources

FinCEN Advisory to Financial Institutions on E-Mail Compromise Fraud Schemes, FIN-2016-A003, Sept. 2016
Business E-Mail Compromise: Cyber-Enabled Financial Fraud on the Rise Globally, www.fbi.gov, Feb. 2017

SECTION 2

Employment Scams

What is it?

***Employment Scams target individuals with the promise of a job** that, typically, involves processing financial transactions for the employer.*

Who are the victims?

Job seekers, college students, underemployed, stay-at-home parents, or retirees may be susceptible to these scams.

How does it work?

Fraudsters will post ads on online forums and social networks such as Craigslist and Facebook, as well as send out emails and text messages to large groups of random individuals, promising high paying jobs that can be done from home.

If the fraudster believes a specific institution has controls that can be exploited, they may request the victim open an account at a targeted institution. Otherwise, the fraudster will use the existing accounts of the victim to conduct the fraud.

The fraudster uses the victim's financial information to either initiate ACH credits or perform mobile deposits to the account. They then instruct the victim to forward the funds into an account the fraudster controls, less a processing/administrative fee that is meant as payment to the victim.

When the unauthorized ACH or fraudulent check returns, the victim is typically held responsible for the loss.

What are the indicators?

- **New clients or clients who are financially vulnerable**. That is, with little access to credit, no or inconsistent payroll, and/or those with a low dollar balance in their account.
- **Mobile deposits or ACH credits that are new** or not typical for the client.
- **Immediate withdrawal or transfer** of funds from the account.
- **Large purchases at locations that process funds transfers**, such as big box stores and international wire processers.

How to mitigate the risk?

- **Account opening procedures probing for possible Employment Scam scenarios** (i.e., Why are you choosing our institution today?)
- **System for real-time detection of unsual deposits and ACH credits.**
- **System displays deposited check images** to allow for timely review by investigators.

Resources
Job Scams, Federal Trade Commission (FTC)
BBB Tip: Employment Scams, Better Business Bureau, Mar, 2017

SECTION 3

Lottery Scams

What is it?

***Lottery Scams promise large lottery winnings** in return for an initial processing fee from the victim.*

Who are the victims?

General public, but typically elderly persons, and those who may be financially vulnerable.

How does it work?

Fraudsters will use mass phishing techniques to identify victims, and lure them in with the prize of a large lottery win.

Victims are requested to forward a processing fee to the fraudster before receiving their winnings.

If the victim does forward a fee, then the fraudster will make additional requests for funds — often under the guise of withholding tax fees or administration fees.

This will continue until the victim catches on or runs out of money.

What are the indicators?

- **Large funds transfer** that is not typical for the client.
- **Funds transfers to international locations.**
- **Large ATM withdrawls.**
- **Large purchases at locations that process funds transfers**, such as big box stores and international wire processers.
- **Client using lines of credit or pulling from investments**, which is out of character for them.

How to mitigate the risk?

- **Training for front line staff to identify individuals who are excited/happy about making a large transfer.** Client may say they just won the lottery or have come into unexpected money.
- **Detection systems that profile both sending and receiving accounts of a funds transfer** to ensure the activity is typical for both parties.

Resources

Five red flags to help you spot a lottery or sweepstakes scam, Better Business Bureau, Sept. 2015

SECTION 4

Online & Payday Loan Scams

What is it?

***A fraud targeting individuals with the promise of a loan** in exchange for a fee.*

Who are the victims?

College students, underemployed, individuals facing some form of additiction (gambling, substance abuse).

How does it work?

Fraudsters will post ads on online forums and social networks such as Craigslist and Facebook, as well as send out emails and text messages to large groups of random individuals.

These ads promise access to loans regardless of credit history or employment status.

Once the victim responds, the fraudster will request financial details from the victim such as account information or online/mobile login credentials.

The fraudster will use this information to either initiate ACH credits or perform mobile deposits to the account with instructions for the victim to then return a portion of the funds as part of a processing fee.

What are the indicators?

- **Mobile deposits or ACH credits that are new** or not typical for the client.
- **Immediate withdrawal or transfer** of funds from the account.
- **Large purchases at locations that process funds transfers**, such as big box stores and international wire processers.

How to mitigate the risk?

- **System for real-time detection of unsual deposits and ACH credits.**
- **System displays deposited check images** to allow for timely review by investigators.

Resources

Advance-Fee Loans, Federal Trade Commission (FTC), Aug. 2012
2016 BBB Scam Tracker Annual Risk Report: A New Paradigm for Understanding Scam Risk, Better Business Bureau Institute for Marketplace Trust

SECTION 5

Romance Scams

What is it?

A fraud that targets victims who may be emotionally vulnerable with companionship and friendship, with the goal of having the victim send funds for travel, medical care, or a business opportunity.

Who are the victims?

Those who are widowed, retired, divorced or are single.

How does it work?

Fraudster will make contact with the victim through social media networks, online forums, or dating sites.

The fraudster is typically located overseas but may portray themselves as an American (military, business professional, etc.).

This fraud may takes months to develop as the fraudster builds trust with the victim.

At some point the fraudster will make a request for money. Typical requests include travel expenses to see the victim; emergency medical expenses for the fraudster or a family member — usually a child; or a business opportunity that will allow them to get enough money to live together.

The fraudster will generally begin by requesting a small amount of money, and increase the requests over time.

What are the indicators?

- **Large funds transfer** that is not typical for the client.
- **Funds transfers to international locations.**
- **Large ATM withdrawls.**
- **Client using lines of credit or pulling from investments**, which is out of character for them.
- **Large purchases at locations that process funds transfers**, such as big box stores and international wire processers.

How to mitigate the risk?

- **Training for front line staff to identify escalating fund transfers** to a relatively new recipient where the amounts are increasing — especially to overseas locations.
- **Detection systems that profile both sending and receiving accounts of a funds transfer** to ensure the activity is typical for both parties.

Resources

Romance Scams – Online Imposters Break Hearts and Bank Accounts, Federal Bureau of Investigation, Feb. 2017

SECTION 6

Who's most at risk?

Is there a *clear* picture?

We tend to think of the elderly as the country's primary fraud victims; however recent studies suggest this belief may not be so clear-cut.

In February 2017, a collaboration between the Stanford Center on Longevity and the Financial Industry Regulatory Authority (FINRA) Investor Education Foundation released the results of a pilot survey to measure financial fraud in the United States. The survey was administered to a sample of 2000 Americans age 18 and older and found the average age of fraud victims across multiple scam types was 41 years old. This finding is in line with an earlier 2011 Federal Trade Commission (FTC) consumer fraud survey which found people between the ages of 45 and 54 were most likely to have been a fraud victim.

While the research results skew younger than many would expect, **it is important to note that everyone is a potential victim**. Additionally, the study found there was no overall fraud victim stereotype, instead there were noticeable demographic differences based on scam type.

Though there is no clear overall victim profile, there are groups that appear to be susceptible to specific scams, as referenced in the previous sections. The emotional impact was clear regardless of scam type.

More than half of the victims in the Stanford study declared the incident was "moderately or severely distressing". When asked specifically about their feelings, respondents used words such as frustrated, used, betrayed, physically ill, and suicidal.

Scams and the Elderly

- Older adults are less likely to acknowledge and report having been a fraud victim.
- Research indicates that age-related declines in cognition are associated with susceptibility to scams.
- The elderly are disproportionately targeted by criminals, likely due to a perceived access to wealth.

"I can't even imagine a man, a person, that could be this bad," *she said. "I can't think of him that way [...] There can't be a man in this world that could be this horrible to have* ***purposefully done what he's done to me."*** [4]

– Romance Scam Victim
Texas, 2017

Resources
Findings From a Pilot Study to Measure Financial Fraud in the United States, Stanford Center on Longevity & FINRA Investor Education Foundation, Feb. 2017
Consumer Fraud in the United States, 2011, Federal Trade Commission, April 2013.

Fraud Scams: Quick Reference Guide

This quick reference guide is designed to help those combating fraud within financial institutions learn about common scam scenarios. Feel free to print and share this page with front-line staff, colleagues, and peers.

SCAM	DEFINITION	VICTIMS	INDICATORS
Business Email Compromise (BEC)	*Targets a business or commercial client in the attempt to initiate a large funds transfer to an account under the fraudster's control.*	CEOs, CFOs, Accountants, Bookkeepers, Accounts Payable	▪ Large wire or funds transfer to a new recipient. ▪ Transfers initiated near end-of-day or cut-off windows; and/or before weekends or holidays. ▪ Receiving account does not have a history of receiving large funds transfers. ▪ Receiving account is a personal account and the company typically only sends wires to other businesses.
Employment Scam	*A fraud targeting individuals with the promise of a job that typically involves processing financial transactions for the employer.*	Job seekers, college students, underemployed, stay-at-home parents, retirees	▪ The client is new or financially vulnerable, has little access to credit, no or inconsistent payroll, and/or has a low-dollar balance in their account. ▪ Mobile deposits or ACH credits that are new or not typical for the client. ▪ Immediate withdrawal or transfer of funds from the account. ▪ Large purchases at locations that process funds transfers, such as big box stores, and international wire processers.
Lottery Scam	*A type of fraud promising large lottery winnings in return for an intital processing fee from the victim.*	General public but typically those who may be financially vulnerable	▪ Large funds transfer that is not typical for the client. ▪ Funds transfers to international locations. ▪ Large ATM withdrawls. ▪ Large purchases at locations that process funds transfers, such as big box stores and international wire processers. ▪ Client using lines of credit or pulling from investments, which is out of character for them.
Online & Payday Loan Scam	*Fraud targeting individuals with the promise of a loan in exchange for a fee.*	College students, underemployed, individuals facing some form of addiction	▪ Mobile deposits or ACH credits that are new or not typical for the client. ▪ Immediate withdrawal or transfer of funds from the account. ▪ Large purchases at locations that process funds transfers, such as big box stores and international wire processers.
Romance	*A fraud that targets victims who may be emotionally vulnerable, with the goal of having the victim send funds to the fraudsters.*	Widows, widowers, retirees, divorcees, singles	▪ Large funds transfer that is not typical for the client. ▪ Funds transfers to international locations. ▪ Large ATM withdrawls. ▪ Client using lines of credit or pulling from investments, which is out of character for them. ▪ Large purchases at locations that process funds transfers, such as big box stores and international wire processers.

CONTACTS

FRAUD/COMPLIANCE CONTACT: _____

POLICE: _____

OTHER: _____

OTHER: _____

NOTES

_____

_____

_____

_____

Verafin is an industry leader in cross-institutional Fraud Detection and Anti-Money Laundering (FRAMLx) collaboration software with a customer base of more than 1500 financial institutions across North America.

With advanced behavior-based analytics, Verafin helps financial institutions stay a step ahead of numerous types of fraud as well as the BSA, USA PATRIOT Act, and FACTA compliance landscape.

Verafin is the exclusive provider of fraud detection and BSA/AML software for the California Bankers Association, Florida Bankers Association, Massachusetts Bankers Association, Texas Bankers Association, Illinois Bankers Association, CUNA Strategic Services, a preferred service provider of the Independent Community Bankers of America, and has industry endorsements in 47 states across the U.S.

Verafin's innovative crime-fighting solutions include FRAMLxchange, the industry's largest secure 314(b) information sharing network, that facilitates collaboration between more than 1100 financial institutions and 3000 investigators, and is available to any 314(b)-registered institution.

For more information, contact Verafin today.

1.877.368.9986
info@verafin.com
www.verafin.com

VERAFIN
A STEP AHEAD