FRAUD PREVENTION FRIDAY

Friday, July 26, 2024

Opt For Layered Identity Verification For Safer, Efficient Digital Operations

A strong verification strategy can help financial services providers build customer trust while still fighting fraud.

A robust verification strategy can help financial services providers establish and maintain customer trust while confirming consumer identity. Accomplishing both is increasingly difficult yet remains critical to conducting business.

With the right tools in place, master digital transformation

GBG's State of Digital Identity Report found that 62% of U.S. consumers said they would be more likely to onboard with a business using more advanced identity verification.

As the world becomes increasingly digital, institutions must master the complexities of digital transformation. Staying competitive means effectively curbing rising fraud while keeping pace with consumer expectations. A layered approach to identity verification solutions can help financial institutions foster trust, empowering them to create more efficient digital experiences.

Top News

- Opt For Layered Identity Verification For Safer, Efficient Digital Operations
- Federal Bureau of Investigation Internet Crime Complaint Center (IC3)
- International Association of Financial Crimes Investigators (IAFCI)
- ICBA/CBM Check Fraud Guide
- W.I.R.E. What I Require Every Time - Wire Fraud Information

Federal Bureau of Investigation Internet Crime Complaint Center (IC3)

We learned at the Risk Fraud Forum this week, it is imperative consumers report all internet crime to the FBI via the IC3 website.

Today's cyber landscape is threatened by a multitude of malicious actors who have the tools to conduct large-scale fraud schemes, hold our money and data for ransom, and endanger our national security. Profit-driven cybercriminals and nation-state adversaries alike have the capability to paralyze entire school systems, police departments, healthcare facilities, and individual private sector entities. The FBI continues to combat this evolving cyber threat. Their strategy focuses on building strong partnerships with the private sector; removing threats from US networks; pulling back the cloak of anonymity many of these actors hide behind; and hitting cybercriminals where it hurts: their wallets, including their virtual wallets.

Critical to the FBI's efforts is the Internet Crime Complaint Center (IC3). IC3 gives the public a direct way to report cybercrime to the FBI and enables us to collect data, advance investigations, and identify changes in the threat landscape. In 2023, IC3 received a record number of complaints from the American public: 880,418 complaints were registered, with potential losses exceeding $12.5 billion. This is a nearly 10% increase in complaints received, and it represents a 22% increase in losses suffered, compared to 2022. As impressive as these figures appear, we know they are conservative regarding cybercrime in 2023. Consider that when the FBI recently infiltrated the Hive ransomware group's infrastructure, we found that only about 20% of Hive's victims reported to law enforcement. More reporting from victims would mean superior insight for the FBI.

International Association of Financial Crimes Investigators (IAFCI)

The International Association of Financial Crimes Investigators (IAFCI) was discussed at length during our Risk/Fraud forum on Thursday, July 25, 2024.

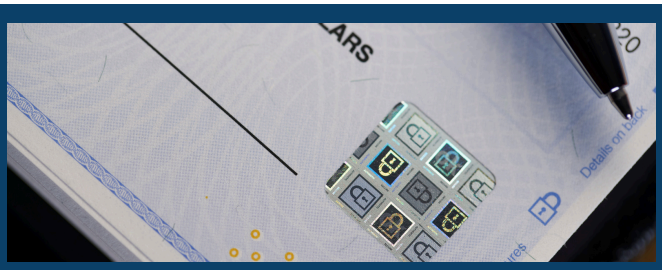
The IAFCI has partnered with a number of community banks in the state to help combat fraud and is a resource the Michigan State Police use to identify and help bring fraudsters to justice. They are a non-profit international organization providing services and an environment where information about financial fraud, fraud investigation, and fraud prevention methods can be collected, exchanged, and taught for the common good.

If you are charged with fighting fraud within your bank, review their site and get involved. Together, we will make a difference in battling back against bad actors everywhere.

W.I.R.E. What I Require Every Time - Wire Fraud Information

Take a look at the Myths and Myth Busters regarding Wire Fraud from CBM Preferred Partner Investors Title

Myth 1 ▶	Using encrypted email is sufficient protection against fraud.
Myth Buster ▶	**NO!** It is not sufficient if you are sending the email to the wrong address or individual.
What to do?! ▶	Check the accuracy of all email addresses!
Myth 2 ▶	Once an email is encrypted it is encrypted forever.
Myth Buster ▶	**NO!** Sending an email through encrypted email does NOT mean that forwards of that email will also be encrypted.
What to do?! ▶	Send wiring instructions directly to the intended recipient. Do not use third parties to relay wiring instructions.
Myth 3 ▶	Wiring Instructions can be trusted if they are received via encrypted email or fax.
Myth Buster ▶	**NO!** Cyber criminals can and do send wiring instructions via encrypted emails and/or fax.
What to do?! ▶	Verify and confirm wiring instructions with the intended recipient using a known, verified telephone number.
Myth 4 ▶	Changes in wiring instructions is the only cause to warrant exercising additional caution.
Myth Buster ▶	**NO!** There are many red flags to watch for.
What to do?! ▶	Confirm **ALL** wiring instructions with the intended recipient using a known, verified telephone number.
Myth 5 ▶	My E&O Insurance will cover me for cyber fraud.
Myth Buster ▶	**NO!** General Liability and E&O Policies generally have exclusions for cyber fraud.
What to do?! ▶	Ask your insurance agent about cyber fraud coverage.
Myth 6 ▶	All Cyber Fraud Insurance is the same.
Myth Buster ▶	**NO!** Not all Cyber Fraud Insurance is alike.
What to do?! ▶	Ask your insurance agent about Cyber Liability Insurance (loss of data) and Cyber Crime Insurance (loss of money). They are two distinct and different types of coverage.



ICBA/CBM Check Fraud Guide

Earlier this year, we shared the ICBA/CBM Check Fraud Guide. Many bankers have requested this, so we are sharing again. This is a handy tool; share it with your team.

This guide is a resource to help community banks both minimize the incidents of check fraud related to altered, forged, and counterfeit checks and take appropriate steps to recover funds or otherwise minimize loss when it does occur.

The guide explains how the laws and regulations governing checks assign liability for check fraud to individual banks involved in the issuance, transmittal, and receipt of checks. In addition, it lists various defenses a bank may raise to avoid liability for check fraud.1 The guide also has three appendices that cover the check fraud landscape, mechanisms for preventing check fraud, and the legal and regulatory regime governing checks.