Preventing Wire Fraud Through Verification

cyber security authentication fraud protection

Summary: Wire fraud is an ongoing problem for CFIs and their customers. Implementing multiple verification methods can help combat this. We explore a variety of options and provide the pluses and minuses of each one.

A reporter and her husband found a house they wanted to buy, but the closing process grew strange. Their title company sent them a series of frustrating emails, insisting that they pay for the purchase via a wire transfer and not the certified check that they preferred. A lucky call to their real estate agent revealed that no one at their title company had ever emailed them. The proposed wire transfer was an attempted cybercrime.

In the never-ending war between digital crime and its prevention, digital crime is winning the aggregate game. The number of attempted wire fraud occurrences against businesses trended up slightly from Q1 2021 to Q1 2022, and those attempts more than doubled in value. As you can imagine, the most targeted industries were finance and insurance, which accounted for 23% of total attempts. Personal wire fraud also continues to be a problem, especially among an older demographic: 68% of wire fraud victims in 2022 were aged 55 and older.

Verifying large transactions, which typically also means verifying the authenticity of the sending and receiving accounts, is a vital part of preventing wire fraud. Like all financial institutions, community financial institutions (CFIs) have a variety of verification options to help protect their customers and employees from wire fraud. Considering the prevalence of wire fraud, it's important for a CFI to stay abreast of the most effective authentication methods — and ideally implement at least one of them.

Although each authentication method will have pros and cons, they can all cover some important bases in protecting your institution and your customers from cybercrime. Here are some of the **top verification methods available right now:**

- An **SMS One-Time Password (OTP)** sends users a one-time code via text message. They enter this code on their mobile banking app within a specific amount of time to confirm the transaction. This method is easy to use, which is why it's one of the most popular verification methods in the banking industry. However, it's also expensive and vulnerable to SIM interception and social engineering attacks.
- **PINs** are a string of four to eight numbers that users enter to authenticate a transaction. Like SMS OTP codes, this is a user-friendly and common method. Weak PINs like 12345, however, are vulnerable to data breaches, and users tend to use overly simplistic and easy-to-guess PINs that leave them open to potential fraud.
- **Hard tokens** are physical security devices that generate single-use PINs. Users have to actually possess the device to authenticate a transaction, so this is a quite secure method. The security, however, is expensive and can involve a lot of work from IT staff, and users can lose the device or may find the system inconvenient.
- **Soft tokens** are software-based tokens that can serve as authentication apps on their own or integrate into a mobile banking app. They can't be lost and they're both less expensive and more convenient to use than are hard tokens. Though they provide strong security, they aren't invulnerable to cyberattacks.
- **Micro deposits** verify customers' information by depositing funds under one dollar into a customer's account, which the customer must then report the amounts of back to the financial institution to confirm

that the receiving account is valid. The deposits will show the sender's identity, demonstrating the funds' source. While easy to use, micro deposits are vulnerable to scammers, particularly with so-called salami attacks, which are a series of small, fraudulent transactions tested against stolen account information to show fraudsters which accounts are valid and vulnerable.

- **Third-party verification services** use multiple authentication methods, including checking databases with negative account history, checking for valid routing and account numbers, or directly confirming information with each individual financial institution. These services are as good as the methods they use and the potential fallibility of each.

It's a fair bet that cyber thieves will continue evolving methods to get around the latest security techniques. However, CFIs have a long list of authentication methods available to protect themselves and their customers from wire fraud, and those options are constantly changing and updating to keep up with cybercrime trends. Although it can be difficult to pinpoint the best authentication method that will suit your customers, your staff, and your budget, keep in mind that some protection is certainly better than none.

ATTRACT NEW CUSTOMERS WITH INTERNATIONAL SERVICES

Help new customers with their cross-border commerce using seamless international services from PCBB. It is like having your own international department on call. Learn more today.

ECONOMY & RATES

Rates As Of: 02/21/2023 12:05PM (GMT-0700)

Treasury	Yields	MTD Chg	YTD Chg
3M	4.84	0.14	0.42
6M	4.99	0.19	0.23
1Y	5.02	0.35	0.31
2Y	4.71	0.51	0.29
5Y	4.17	0.56	0.17
10Y	3.95	0.44	0.08
30Y	3.97	0.34	0.01
FF Market	**FF Disc**		**IORB**
4.58	4.75		4.65
SOFR	**Prime**		**OBFR**
4.55	7.75		4.57