Truth Behind the Numbers: Transaction Fraud

How Much Is It Costing Your Financial Institution and What You Can Do

Alogent

OVER 50% OF FINANCIAL INSTITUTIONS HAVE FALLEN VICTIM

Fraudulent activity in the banking market is rapidly evolving. Cybercriminals are relentlessly looking for weaknesses in systems to scheme against consumers, businesses, and the financial institutions themselves.

According to a 2022 survey from the Association for Financial Professionals, 71% of banks and credit unions have been victims of attempted payment fraud. While payment fraud has always been a significant financial detriment to institutions, the associated costs to remedy this breach continue to climb.

But it is not all doom and gloom - technology continues to become more advanced, and solution providers are offering banks and credit unions more opportunities to fight back – as well as stay ahead of fraudsters by leveraging insights around trending fraud types and best practices.

FRAUD ON THE RISE

Financial institutions of all sizes continue to see an increase in the number of overall fraud attempts, and according to research, this can be upwards of 1,875 attempts a month in the US alone. Although the number of blocked attempts is high, just one successful fraud attack can cost a bank or credit union thousands, if not millions, of dollars in losses and recovery.

If we look specifically at check fraud, criminals have given new life to this old scheme in recent years. With recent emphasis placed on cyber security and digital payments, fraudsters have taken the opportunity to exploit protection gaps within the postal system. “Mail fishing” (also known as “mail theft”) occurs when individuals steal checks from residential mailboxes, cluster box units or USPS blue collection boxes – this includes personal checks, business checks, tax refunds, and government benefits.

There have also been reports of mail carriers being targeted while on their delivery routes. After stealing the checks, criminals make alterations in a process known as "check washing." Using household chemicals, the courtesy amount (CAR) and legal amount (LAR) fields, as well as the payee name, are often changed.

According to the Financial Crimes Enforcement Network (FinCEN), in 2022 the number of reports of potential check fraud reached over 680,000 filings, up from 350,000 in 2021.

It is important for banks and credit unions to realize that check fraud is not limited to only physical (paper) channels, but crosses into digital channels, as well. "Duplicate check fraud," or "duplicate deposits," is rising with the use of remote deposit capture (RDC). After an individual deposits a check via their mobile device or a remote scanner, the physical and signed check is still in their possession, which is when criminals take the opportunity to cash the already deposited check at another location – doubling their funds.

DIGITAL FRAUD TRENDS

In addition to check fraud, there are newer fraud techniques impacting the financial services sector. Digital banking and digital transformation efforts are a common priority for organizational leaders, and according to TransUnion's global online fraud trends analysis, digital fraud attempts have spiked by 22% in the United States, and 46% worldwide since the start of the pandemic.

With efforts to stay ahead of the fraudsters, leaders must be knowledgeable about best practices within their sector and how the problem, and technology, are evolving. DataVisor notes the following schemes for bank and credit union leaders to be aware of:

Identity theft – targeting the onboarding process, fraudsters steal personal identifying information, like social security numbers, and create "synthetic identities" to open new accounts at other financial institutions.

Account takeovers – phishing methods, like email or text, convince consumers to click on links which give fraudsters access to passwords; they are then stolen and used to get into digital accounts and drain them.

Transaction fraud – after stealing credentials, criminals log in to popular platforms like Venmo or Zelle to siphon funds. ACH fraud is also a growing concern, as it is easy to commit with checking account and routing number details.

Cybercriminals may work individually or in a fraud ring for more sophisticated and ongoing schemes. They are smart, tech-savvy, and continue to modify their methods, looking for any point of vulnerability to gain access. And while techniques shift, so does access to funding, which creates an even riskier combination for financial institutions and their account holders to establish preventative measures against it.

THE COST OF FRAUD TODAY

The cost of fraud continues to surge. LexisNexis reports the value of fraud for U.S. institutions is upwards of 10% higher today than pre-pandemic levels. Behind every instance of fraud are hidden costs beyond the value of the transaction itself, including fees linked to labor and investigations, and legal and recovery expenses, causing even greater losses for banks and credit unions.

Every $1 lost to fraud costs a financial services organization as much as $4.23, compared to $3.64 in 2020 – a 16.2% increase.

Cost of Fraud: U.S. Financial Services

Year	Dollar Increase
2019	$3.25
2020 pre-pandemic	$3.64
2020 during pandemic	$4.12
2021	$4.00
2022	$4.23

**source: LexisNexis Risk Solutions, 6th Annual True Cost of Fraud™ Study: Financial Services and Lending Report, U.S., and Canada Edition 2022*

To put these amounts in perspective, a $5,000 fraud loss can cost a financial institution $21,150!

In the case of check fraud, expert analysts estimate that damages from check fraud are expected to reach as high as $24 billion in 2023, which is about a 50% increase from 2018 – even though check utilization is decreasing.

THE COST OF ACCOUNT HOLDER CHURN DUE TO FRAUD

With every fraud attempt comes the risk of account holder churn. A 2022 Aberdeen Strategy & Research study reports that nearly 75% of retail bank accounts fall victim to an account takeover (ATO) crime annually, which causes about one-third of their account holders to leave their primary institution and bank elsewhere – causing lost revenue.

Since it's estimated to be 5-times more expensive to onboard a new account holder than to retain one, this is just one additional reason to stay ahead of best practices. Ultimately, unsuccessful fraud mitigation is detrimental to the future growth of an institution.

START TAKING ACTION AT YOUR FINANCIAL INSTITUTION

With costs like these, it's no surprise that the banking industry has adopted new techniques, many of which rely on AI and machine learning-based capabilities to keep fraud at bay across all points of presentment – including at self-service locations and devices used outside the branch. In addition to new approaches and bots leveraged by the fraudsters, banks and credit unions must also assess a potential increase in vulnerabilities linked to consumer behavior and new devices entering the banking landscape.

Within the check fraud space specifically, it's crucial to ensure recognition engines are kept up-to-date and tuned appropriately for all types of checks, including on-us images – a large source of recent fraud. Fraud mitigation capabilities must address the uniqueness of these images, including the ability to interrogate:

- Image quality (IQA) and Image usability analysis (IUA)
- Check stock validation
- Amount recognition and mismatch (CAR and LAR)
- Date
- Payee and Payor name
- Check number
- MICR codeline
- Signature detection and verification

The difficult reality for banks and credit unions is that fraud can occur at any step in the user journey and from any device or workflow, making it nearly impossible to pinpoint a one-size-fits-all solution to the still growing problem. Addressing the issue is even more complicated, as institutions must balance the total cost of fraud losses with security and protection solutions, all without sacrificing the user experience. In the end, a holistic, multi-faceted approach that combines best practices and cutting-edge technologies can help protect both your institution and your account holders.

Fraud techniques are constantly evolving. To protect themselves and their account holders, banks and credit unions must work in partnership with their solution providers to stay well-informed of new approaches, including leveraging the latest intelligence from fraud management databases, as well as best practices that secure their transaction ecosystems cross-channel, like:

Combating fraud at the point of presentment: Financial institutions can embrace banking platforms with integrated fraud detection capabilities that monitor and detect potential risks - both with incoming transactions and at the point of presentment. In addition, banks and credit unions that leverage analytical data to observe patterns across all channels can identify anomalies faster.

Doing your due diligence: Not all solutions are designed the same. Doing due diligence allows financial institutions to take a more proactive approach and select the right solutions to meet their needs. Ensure that your chosen solution is equipped with real-time alert capabilities and is built with best practices in mind, keeping your account holders and institution safe.

Training and educating staff and account holders: Staff training and account holder education are equally important and must be leveraged in combination with fraud detection engines. Topics like the importance of regularly changing passwords, enrolling in multi-factor or biometric authentication, and other best practices have been said to stop nearly 99% of cyber-attacks.

ADDRESS FRAUD WITH ALOGENT PAYMENT SOLUTIONS

Alogent's end-to-end deposits automation solutions, combined with the latest fraud mitigation techniques and engines, secure your enterprise payment channels across all points of presentment and the back office - reducing losses, and ensuring a consistent and simple UX for your account holders. Combat fraud before the transaction enters your workflows and keep your payment ecosystems secure.

Scalable, cloud-ready solutions for branch and teller capture, remote deposit capture, merchant capture, image-enabled ATMs & ITMs, and back office processing.

Unify - Alogent's patent-pending cloud-native, thin-client image acquisition and processing platform, takes your payments infrastructure to the next level of convenience, efficiency, and security.

With a single API, your bank or credit union can leverage the same platform across all of your deposit channels - in the branch, the back office, and remote. Every application and point-of-capture accesses one database and reporting dashboard, delivering a clear and centralized view into all transactions, deposits, the statuses of the items downstream, points and trends of check fraud, and more.

- Open banking platform driven by a single set of code and just 1 API
- Tight integrations to third-parties
- Exponential scalability, reduced IT overhead, and a lower cost of ownership with a cloud-native architecture
- Flexibility with common and customized business rules
- Consistent UX across all payment channels with real-time image and data validations
- Browser and operating system agnostic: Windows or Mac, Chrome, Edge, Firefox, Safari, and any combination
- Integrations with AWARE for enterprise-wide data analytics, business intelligence and visual dashboards

ABOUT ALOGENT

Alogent provides proven, end-to-end check payment processing, digital, online, and mobile banking, enterprise content and information management, and tracking and exception management solutions to financial institutions including credit unions, community banks, and some of the largest national and international institutions. Our unique approach spans the entire transaction "ecosystem" —from capturing and digitizing transaction data, to automating entire transaction workflows and making information available across the enterprise. Alogent's solution suites leverage the latest in AI, machine learning and predictive analytics, enabling financial institutions to deliver products and services that boost engagement through personalization and data-backed decisions.

Learn more about Alogent and Unify, our patent-pending, single API, and cloud-native solution, at alogent.com/payment-solutions/unify.