

Rethinking Check Fraud: Taking a New Approach to an Old Fraud Type



Andy Schmidt

Research Director, Global Payments
November 2010

Executive Summary

Check fraud was the most common type of deposit account fraud in the United States in 2008, accounting for more than 50% of all deposit account fraud volume. Because check fraud totaled "only" \$1 billion (USD) in losses on \$41 trillion in check volume, many banks view check fraud as a cost of doing business.

TowerGroup believes that actual fraud losses are as much as 50% higher than reported because of the difficulty in distinguishing between illicit and accidental behavior in areas like check kiting or dual presentment. Furthermore, the barrier to entry for check fraud is extremely low, while the technical sophistication is increasing dramatically as evidenced by attacks on check image repositories. New, flashier fraud types distract banks, customers, and regulators, creating a perfect hunting ground for check fraudsters. TowerGroup believes the best approach to reducing check fraud combines teller training and image technology with back-end analytics, which holds the greatest promise of stemming, if not reversing, the overall growth in check fraud losses.

Overview

According to the American Bankers Association (ABA), deposit account fraud accounted for more than nearly \$2 billion (USD) in losses in the United States in 2008 as fraudsters attacked via check, debit card, and Automated Clearing House (ACH). Check fraud, the most prevalent deposit account fraud type, accounted for nearly half of this total yet receives little attention compared to its impact on the bank's bottom line.

This TowerGroup report examines the reasons that check fraud loss is growing in the United States despite technological advances in fraud prevention. The report then outlines the benefits and drawbacks of the approaches many US financial services institutions (FSIs) are taking to shift from a reactive to a proactive stance in addressing fraud overall.

Analyzing US Check Fraud

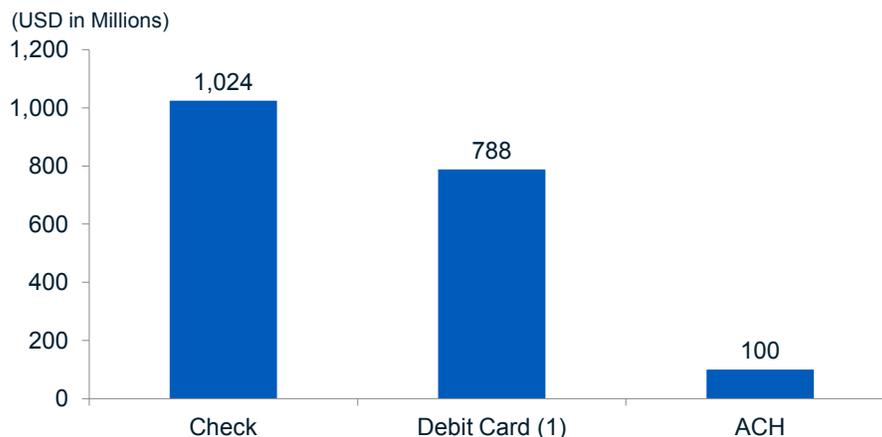
"Despite law enforcement's very necessary focus on combating serious and organized financial crime, including terrorist-related activities that remain an ongoing threat — one of the simplest and most prevalent ways to commit a financial crime, to steal money, is to commit some form of check fraud." *—James H. Freis, Jr., Director, Financial Crimes Enforcement Network (FinCEN), US Department of the Treasury, October 2, 2010.*

Check fraud is one of the oldest types of deposit account fraud. According to the American Bankers Association's *2009 ABA Deposit Fraud Survey Report*, check fraud amounted to \$1,024 million in 2008, a 6% increase from the 2007 ABA survey, with 80% of banks reporting some form of check fraud in both surveys. This made check fraud the greatest source of deposit account fraud in the United States, as shown in Exhibit 1.

Exhibit 1



US Deposit Account Fraud (2008)



Source: American Bankers Association, Federal Bureau of Investigation, TowerGroup
(1) For debit by point-of-sale (POS) signature, POS personal identification number (PIN), and automated teller machine (ATM).

Fraudsters Commit Check Fraud Because It's Easy

Check fraud, which is the illegal use of checks to obtain funds from a deposit account, takes many forms:

- **Counterfeiting**, creating a fake check (e.g., via desktop publishing)
- **Forging**, signing a check without authorization
- **Kiting**, playing the float between the time the check is deposited by the recipient and sufficient funds become available in the maker's account
- **Paperhanging**, writing checks on a closed account
- **Washing**, using chemicals to remove ink from a check to change the payee and/or legal amount

This list underscores the fact that the barrier to entry is remarkably low since the information needed to commit check fraud can be obtained from a variety of sources. Fraudsters can find discarded bank account statements in the trash or buy account information online as well as purchase standard check stock at their local office supply store and use desktop publishing applications to create official-looking yet phony checks.

Check fraud is becoming increasingly sophisticated as fraudsters use malware like the Zeus Trojan to steal online banking credentials, which they use to gain account access. Once they gain access to an account, they either change the account address and order new checks to draw on the account or use the routing numbers to create counterfeit checks to draw on the account.

In an example discovered in 2010, a Russian check fraud ring broke into check cashing services and corporate databases to steal check images and information, including the checks' routing number and account numbers as well as the company name and address and the image of the authorized signature. Using this method, the ring generated over 3,000 checks totaling about \$9 million (at approximately \$3,000 per check) over a 12-month period. This per-check average is much higher than average amount of check fraud of approximately \$1,350 per check reported by the ABA.

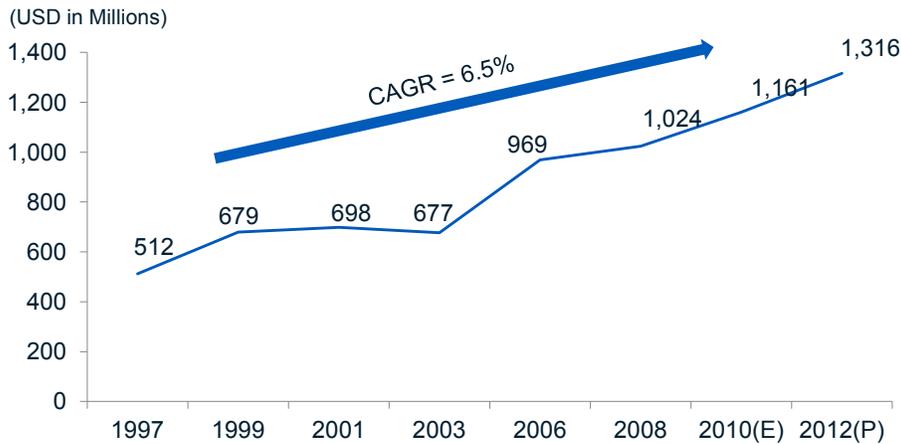
Given the simplicity and growing sophistication of check fraud, TowerGroup projects that *reported* check fraud in the United States will top \$1.3 billion by 2012. We believe the actual *total* amount of check fraud may be as much as 50% higher than the reported figure, but the difficulty of distinguishing between illicit and accidental behavior in areas like check kiting or dual presentment makes it hard to confirm the actual amount.

The projected level of reported check fraud through 2012 reflects the compound annual growth rate (CAGR) of 6.5% exhibited by check fraud since 1997, a pace more than double the rate of inflation for the period. Historical and projected reported check fraud losses are shown in Exhibit 2.

Exhibit 2



Reported US Check Fraud Losses (1997–2012P)



Source: American Bankers Association, TowerGroup

Large Checks Remain Popular in Some Segments

Even though check volumes are falling steadily in the United States and globally, Americans still wrote more than 26.6 billion checks in 2008, a figure TowerGroup believes will fall to 18.7 billion by 2012, representing a decline of nearly 8.5% per year. While transaction volumes continue to fall, average check *value* continues to climb, having risen 29% from \$1,190 in 2004 to \$1,536 in 2008, making checks the only US payment type consistently increasing in value on a per-item basis. This increase is the result of the migration of smaller, primarily consumer, payments to more convenient electronic payment channels like cards and ACH.

For years, banks have been trying to encourage their business clients to migrate from paper to electronic payment methods because of the greater speed and lower cost of electronic transactions. They have spent millions of dollars creating electronic payment capabilities to serve the business-to-business (B2B) segment. Despite these efforts, adoption still lags in many geographies and segments. As a result the US check system is turning into a high-value, somewhat ignored, paper-based payments channel — the perfect target for fraudsters.

Are the Banks Paying Attention?

"It can be easy to lose sight of the volume of this basic and longstanding type of criminal activity . . . when we compare it to emerging threats to our financial system" —James H. Freis, Jr., Director, FinCEN, US Department of the Treasury, October 2, 2010.

Losing Sight of the Problem

Prevention of check fraud shares the same fate as checks in general: It is not a high priority for many banks. This is because banks prioritize their fraud prevention efforts based on the amount of the loss suffered on an annual basis and the impact that loss has on public and

market sentiment, and by extension, the bank's reputation. At just over \$1 billion in losses in a \$41 trillion industry (0.003% of US check value) in 2008, the cost of check fraud is seen by many bankers as a cost of doing business. In addition, banks see check fraud as simply ordinary, while new and emerging fraud types like account takeover, against which banks have less effective defenses, receive a disproportionate amount of banks' attention because of their adverse impact on public perception and their ability to generate negative media coverage. Bankers perceive these newer fraud types to be exotic and thus more dangerous than check fraud. They assume incorrectly that banks may be more vulnerable to emerging fraud types than to existing types, given the newness of the threat.

Banks' attitude toward check fraud leaves accountholders especially vulnerable, given that no specific protections are afforded to check fraud victims, nearly three-fourths of whom are consumers, according to the ABA study cited above. This situation differs dramatically from the situation for consumers who are victims of unauthorized electronic funds transfer, who are victims are afforded protections by Regulation E. Although as a matter of policy, banks typically make accountholders whole when a counterfeit check is written, they typically hold accountholders liable when they deposit fraudulent checks whether or not they knew the checks were fraudulent. This lack of protection for consumers in checking may be one of the many issues addressed by the newly formed Bureau of Consumer Financial Protection.

Another challenge is that check fraud prevention and investigation can be highly inefficient activities, fraught with static lists, manual processes, and nuances that frequently result in high false positive rates. Consider the example in which a bank customer deposits a check at an ATM that is not image-enabled and the check bounces. If fraud is suspected, the investigator needs to examine a number of factors: Did the payee write the correct amount on the deposit slip? Did the payee key in the correct deposit amount at the ATM? If the person wrote or keyed in the wrong amount, was it a simple transposition error? Do the worded and numerical values for the check amount match? Does the payer simply have messy handwriting? Did the payer have funds in the account when he or she wrote the check? If the person didn't have the funds, did something happen to make the funds unavailable (e.g., late automated payroll deposit, automated bill pay error). These permutations can make check fraud investigation an expensive and manually intensive process that further reduces attention to checks as a payment type because of advancements made in automating ACH and debit card transaction analysis.

This is not to say that check fraud is the fault of banks. The reality is that consumer sentiment and the regulatory or even political attention it can elicit forces banks to choose between combating one type of fraud that they understand and multiple types of fraud that they do not. As is true of many issues, the "squeaky wheel" of emerging fraud types attracts the "grease" of bank attention. Compounding the problem is a lack of hindsight in assessing the impact of fraud prevention programs to determine whether banks are overemphasizing spending on new fraud types instead of preventing old, stable, fraud types that are becoming increasingly preventable with advancements in process and technology (which are discussed in the following sections).

Fraudsters Like Fragmentation

Contributing to this disjointed approach is the lingering belief in many financial services institutions that every payment type is different and thus should be managed separately. As noted in TowerGroup Research Note V64:06PGEW, *Enterprise Risk Management for Payments: Knock the Silos Down*, this notion leads to financial crime prevention being single-threaded in a world where payment fraud increasingly encompasses multiple payment types. The environment is thus ideal for fraudsters to develop and refine their attacks in relative

solitude within a single line of business, later deploying these attacks across the bank's entire footprint.

Shifting from Reactive to Proactive Attention to Check Fraud

The good news is that while over \$1 billion in check fraud losses were incurred in 2008, more than \$11 billion in losses were prevented through a combination of factors as banks of all sizes shift from a reactive to a proactive approach to check fraud prevention. Banks have been able to minimize check fraud through a combination of teller training, image technology, and back-end analytics that enable them to automate and expedite their efforts.

Stopping Fraud at the Point of Presentment

Check fraud is a race against time that begins once the check is presented for deposit or payment. Banks race to verify whether the check is valid, holding funds for as long as possible, while fraudsters rely on the bank making at least some of the funds available while waiting for the total amount to clear.

The Good. Stopping fraud at point of deposit requires a combination of people, training, and image technology. The benefit of this approach is that imaging the check at time of deposit — whether done at the counter by the teller or at an image-enabled ATM — provides the bank a valuable head start in determining whether a check is fraudulent.

Many banks are also training tellers how to physically examine checks while the payee is still at the teller window, providing an added layer of protection that check scanners cannot duplicate. This examination allows the teller to determine whether the check looks "right" and flag a suspicious transaction and possibly escalate investigation even before the transaction is completed.

The Bad. Despite the benefits, this approach has a significant and potentially fatal flaw: teller turnover. In Research Note V55:15R, *The Role of the Bank Teller: What Really Needs to Change?*, TowerGroup estimates teller turnover to average 33% per year, being higher for part-time tellers (53%) than for full-time tellers (approximately 25%). Also discussed in that Note is teller training. Training is one of the key drivers of employee retention for tellers, since those who are adequately trained tend continue working at the job much longer. Retention is especially important if the teller's job includes scanning checks both visually and electronically prior to deposit to combat check fraud because a lack of training leads to inconsistent completion and higher turnover, a phenomenon that fraudsters and their cohorts can easily observe from the bank lobby or the sidewalk outside the bank's windows.

The use of image-enabled ATMs provides an automated solution for checking whether the check amount and deposit amount match.

The Ugly. Because image-enabled ATMs are not ubiquitous, fraudsters can simply avoid them. Furthermore, the images these ATMs print on the transaction receipt provide valuable information to would-be fraudsters, who can obtain receipts by rooting through a person's garbage, or more simply, by picking up a discarded receipt on the street. Even though the receipt may obscure the account number and routing information of the deposited check, the check number, name and address of the payer, name and logo of the payee's bank, and the payee's signature are often clearly visible along with the check amount. Fraudsters can use this information to obtain the payee's account number via social engineering and create checks that look like (and are made out for similar amounts as) checks that have already been paid by the bank.

Using Technology to Look for Patterns After Presentment

Sophisticated analytics that initiate once a check has been deposited rapidly transform check fraud prevention from manual art to digital science and provide the greatest promise in the struggle against check fraud. Many check fraud solutions can identify whether the check is a duplicate, comes from a different checkbook, or is out of sequence and whether checks are being drawn on an account faster than the normal velocity of transactions for that particular account. These solutions incorporate the ability to use business rules and even observed client behavior as filters to reduce the number of cases to be investigated in greater detail.

Because not all check fraud attempts are the same, rules and filters also enable banks to prioritize potential fraud items by risk type, risk level, and transaction amount so their investigators can focus on the items that may have the greatest impact. Although this may sound simple, the impact can be dramatic. TowerGroup has spoken with banks that have used filters to reduce their false positive ratios from upwards of 1,200:1 to a more manageable and realistic 80:1 while still reducing their total check fraud losses.

The smaller number of anomalous checks and transactions can then be examined in much more detail than would have been feasible with a far larger number of checks, even allowing fraud investigators to examine individual check images to compare "good" checks to potentially fraudulent ones. Pairing these capabilities with a case management feature in the check fraud solution allows investigators to keep all of their notes and activities on a case within a single record and hand off or escalate cases as needed. Over time, this case data can be mined to provide FSIs with insights that contribute to the further refinement of business rules and strategies in the battle against check fraud. Vendors to follow in the check fraud market include Actimize, Carreker (Fiserv), Fair Isaac, Memento, Norkom Technologies, SAS Institute, Wolters Kluwer, and Yellow Hammer (Jack Henry & Associates).

Are Incentives Correctly Aligned?

TowerGroup estimates that FSIs in the United States spent \$556 million on check fraud solutions in 2008 and will spend \$718 million per year by 2012 in response to this growing problem. That is approximately 55 cents of prevention for every dollar lost. Millions more are being spent on teller training to curtail fraud at the teller counter.

A piece of the fraud prevention puzzle seems to be missing, however, in that much of this spending perpetuates the old view of check fraud loss as a budgeted expense. This perspective sets a high threshold for acceptable check fraud losses and gives all the attention to new, unbudgeted threats. The dissonance creates an atmosphere in which check fraud investigators have little incentive to improve their approaches and processes.

Managing check fraud more actively — as a figure to be minimized rather than allowed — yields two key benefits. The first is immediate: motivation for staff to actively manage fraud losses because they can see the impact their efforts have on the bank's bottom line. The second is longer term: the ability to allocate savings to minimizing losses via emerging fraud types.

Aspirational Goal: Enterprise Fraud Management

The analytics and case management capabilities of today's check fraud prevention solutions move banks toward the aspirational goal of enterprise fraud management. Such an integrated, firmwide approach pulls fraud prevention and investigation and activities out of the individual payment silos and into a common infrastructure where payment fraud can be addressed in a consistent manner across payment types and geographies.

For some banks, the vision and architecture needed to implement enterprise fraud management equate to an undertaking too massive and challenging to implement. Those willing to undertake the challenge understand that implementing enterprise fraud management is not a "rip and replace" exercise. Instead, it involves the creation of common infrastructure elements that build the bank's capabilities over time. Virtually all top 10 banks are at some point along this evolutionary path, implementing, piloting, or at least investigating a fraud management approach. Midtier banks are also examining the benefits of enterprise fraud management in the payments space because they realize they are the next stop for fraudsters unable to penetrate the top-tier institutions. Key vendors in the antifraud and enterprise fraud management marketplace include Actimize, Detica, Fair Isaac, Fiserv, Memento, Norkom Technologies, SAS Institute, and Wolters Kluwer.

Conclusion

Deposit account fraud is a constant problem for financial services institutions worldwide. Check fraud accounted for more than \$1 billion in reported losses in the United States in 2008. Although the problem may seem small, given the annual dollar volume of checks processed in the United States, fraudsters are seizing upon the banks' lack of attention to the issue by increasing the sophistication of their attacks in order to seize more spoils. These activities contribute to the continued growth in check fraud, which TowerGroup finds troubling, given that check volumes have been falling for years.

As banks shift from a reactive to a proactive approach to check fraud prevention, they must be sure to use a flexible and robust check fraud solution to shore up the potential shortcomings in their focus on teller training and check imaging at point of deposit. Such solutions will allow banks to fight fraud more efficiently by applying sophisticated analytics to discern between accidental and illicit activity, reducing false positive rates while also reducing check fraud losses. By doing so, banks can move past static business rules and filters to make meaningful reductions in annual check fraud losses within their own institutions and across the industry as a whole.



Memento, Inc., commissioned TowerGroup to conduct independent research and analysis of data management practices and trends in financial services. The content of this report is the product of TowerGroup and is based on independent, unbiased research not tied to any vendor product or solution. Although every effort has been taken to verify the accuracy of this information, neither TowerGroup nor the sponsor of this report can accept any responsibility or liability for reliance by any person on this research or any of the information, opinions, or conclusions set out in the report.