WHITE PAPER.

Is Your Check 21 Implementation a Fraud Hazard?

Three financial security experts explain how Check 21 implementations can lead to spectacular fraud detection failures and discuss steps to mitigate the risk.

- Consulting.
- Systems Integration.
- Outsourcing.
- Infrastructure.
- Server Technology.

UNISYS

Imagine it. Done.


UNISYS
Imagine it. Done.


FRANK W. ABAGNALE


41st Parameter

The implementation of the Check Clearing for the 21st Century Act ("Check 21") in the U.S. means that check-handling and collection will experience a drastic increase in speed, but it also portends other seismic issues in the financial services industry — some that are especially foreboding.

First, converting paper checks to digital image has the unintended consequence of significantly reducing the bank's recourse to fraud. Because the image-processing procedure typically involves the destruction of the paper document, eliminating the very evidence of fraud, it could make it extremely difficult to prosecute check-fraud crimes in the future.

Because digital items lend themselves to rapid retrieval, transmittal, and storage, converting to digital opens the door to mass compromise, should these images ever be accessed.

Further, because digital items lend themselves to rapid retrieval, transmittal, and storage, converting to digital images opens the door to mass compromise, should these images ever be accessed. If the wave of recent phishing attacks (spoof email campaigns) is any indication, such large-scale fraud is a very real possibility.

In this collaborative white paper, three fraud experts from the financial services industry discuss the convergence of Check 21, phishing and account takeover scams. They describe the emerging risks, and share their perspectives on possible approaches for banks to adopt to protect themselves—and their customers — against a potential new wave of fraud.

About the Experts

Frank W. Abagnale is a noted author, lecturer, and consultant, and a respected authority on the subjects of forgery, embezzlement and secure documents. For over twenty-five years Abagnale has lectured to and consulted with hundreds of financial institutions, corporations and government agencies around the world. He was also the subject of the major motion picture, "Catch Me If You Can," directed by Steven Spielberg.

Ori Eisen is CEO and President of Phoenix-based The 41st Parameter, which has developed some of the industry's most advanced fraud prevention systems for protecting Internet, mail-order and telephone-order merchants against fraud. Eisen served as the Worldwide Fraud Director for American Express focusing on Internet, MOTO and Counterfeit fraud.

Elazar Katz is director of the Active Risk Monitoring Practice at Unisys. Katz specializes in the rapidly growing field of cross-channel risks and the real-time countermeasures required to address large-scale fraud attacks. Katz meets regularly with bankers worldwide and brings a global perspective to emerging fraud trends. Katz is currently participating in the Financial Services Technology Consortium's Counter-Phishing task force and has been quoted and published in numerous publications.

Identifying the Risks

Frank Abagnale: Check 21 legislation provides the right, but not the requirement, to convert paper checks into electronic images. While Check 21 will significantly speed the handling of checks, it also introduces significant risk and liability to the converting bank because it contains an indemnity that allows a paying bank to charge back a loss resulting from receiving a substitute check rather than the original check. Financial institutions that choose to convert paper checks to digital images assume considerable risk and liability.

Elazar Katz: An indirect, but significant risk stems from banks' plans to post the captured images online as a service to customers. While this seems a relatively benign move, it has profound cross-channel implications. Placing digital check images online effectively opens an electronic access channel to information that previously was available only in paper format. As recent phishing attacks demonstrate, the potent combination of electronic access and computer automation can place thousands of accounts at risk overnight.

Ori Eisen: I agree. In fact, I believe that online banking introduces the single most significant exposure to large-scale account takeover and check-fraud. Beyond the speed and fraud-automation enabled by on-line channels, the Internet also provides anonymity. There's a cartoon from *The New Yorker* being distributed in risk management circles that shows a dog busily clicking on a computer keyboard. The caption says, "On the Internet, nobody knows you're a dog."

Placing both check images and monthly statements online offers fraudsters intelligence on both the visual aspects of the checks and the behavioral history of the account.

Abagnale: Placing both check images and monthly statements online offers fraudsters intelligence on both the visual aspects of the checks and the behavioral history of the account. This type of aggregated intelligence would significantly enhance fraudsters' ability to create counterfeit checks that circumvent both behavior-based and image-based detection systems, should the customer's log in credentials be compromised. As recent phishing scams indicate, large-scale compromise of customer credentials is a very real possibility.

Katz: That's an interesting observation with an even broader implication. In most financial institutions, each business unit develops its own online offerings with little overarching attention to the combined risk impact. Such impact can be significant and unforeseen as electronic speed and convergence of services simplify fraudsters' access to multiple channels and accelerate the speed by which large-scale, mass-produced attacks can be carried out.

Eisen: Much has been discussed recently about phishing — the exploitation of large-scale spoof email campaigns to steal customers' login credentials. Recently, we have come across check-fraud versions of this scam, attributed to gangs from Eastern Europe. The scam involves the following stages:

1. A spoof emailing campaign is launched with the purpose of tricking bank customers to disclose their user name and login passwords
2. Using the fraudulently-obtained user names and passwords, the fraudsters retrieve customers' monthly statements and check images.
3. Using this intelligence, the fraudsters create high-quality counterfeit checks that are nearly identical in appearance, drawn for an amount that is appropriate for the account, and bears a scanned signature.

The potential for mass production of fraud is staggering. In the last 12 months, 57 million US adults received phishing emails, of which 11 million remember clicking on the provided links, and 1.78 million provided passwords and other sensitive personal information.

The potential for the mass-production of this type of fraud is staggering. For example, a recently published Gartner report estimates that in the last 12 months, 57 million U.S. adults received phishing emails, of which 11 million remember clicking on the provided links, and 1.78 million provided passwords and other sensitive personal information. In total, the scams resulted in fraud losses of $2.4 billion.

Abagnale: Another challenge that will face image-based detection systems stems from the limitations of current check readers. Check 21 legislation requires that the converting financial institution provide warranties that the substitute check includes all the information contained on the original check. Since existing check readers can only scan at resolutions approaching 240 dpi while even consumer-grade printers and copiers operate at 600 dpi or above, existing check readers are inherently unable to distinguish between the appearance of an original item or a copy reproduced on such equipment.

Eisen: We've started talking about Check 21 and ended talking about phishing. Many practitioners see phishing as a symptom of today's emailing infrastructure but the problem is really more profound. Although improving today's email infrastructure is important, the problem of large-scale account take over would not be fully resolved. Already we are seeing increased use of key-logging malware (malicious software) and Trojans that transmit back to the fraudsters screenshots of the invaded computer.

Addressing the Challenges

Abagnale: I believe that Check 21 does not diminish the value of security features. While the search for image-survivable security features continues, the only solution that protects both the banks and their customers is one that makes it possible to recognize a fake when it is presented. Banks should encourage customers to use high-security checks with eight or more security features and offer such checks to their business and consumer customers. Also, remember that converting to image is an option not a requirement. The decision regarding which checks to convert should include risk considerations. Banks should also recognize the risk implications of placing check images online and think of ways to mitigate the impact of large-scale compromise of log-in credentials.

Katz: To address the risks of the online channel, a multi-layer defense approach makes the most sense to me. One layer would focus on detecting the phishing attack itself, the next would monitor for suspicious online intelligence-gathering sessions, and the last would focus on detecting the counterfeit check itself. This approach would be particularly effective if the various layers could communicate and alert each other of incoming fraud scams.

Despite the anonymity provided by the Internet, there are multiple parameters that earmark a suspicious session.

Eisen: Despite the anonymity provided by the Internet, there are multiple parameters that could earmark a suspicious session. This approach is effective regardless of the business line, involves no customer action or thought, and is transparent to customers as well as fraudsters. The less you have to involve the customer in your security measures the better. Requiring the customer to take an active part in the solution is problematic since it may lower adoption rates, confuse some users, and even weaken the bank's brand (since it reminds customers of the inherent security weakness of the channel).

Katz: Session analysis can be even further enhanced by combining it with real-time monitoring for atypical usage patterns and known fraud scams. The key is to let the various detection systems share their findings and collaborate in analyzing situations as they emerge. The approach must also be holistic, combining information from multiple channels — implementing additional isolated detection systems won't work.

Eisen: True. Combining knowledge to enhance detection holds true not only across channels but within each channel as well. When analyzing the suspiciousness of an Internet session, for example, we analyze the situation from multiple angles — the source IP address, the PC configuration, the type of activity, and so forth.

Planning for the Future

Katz: In an increasingly connected, global society, one in which fraudsters can strike anytime and anywhere, active, reliable protection against sophisticated fraud schemes is a business imperative — an essential element in any financial services organization. It's become clear that some of the very aspects of Check 21 that will save banks time and effort in check processing also have the potential to provide yet another avenue by which criminals can perpetrate fraud. Looking into the future, how will the threat landscape evolve and what should banks do to prepare?

Abagnale: In the area of check security, significant work will have to be done to develop new forms of image-survivable security features. Also, recognizing that fraud is becoming a multi -channel issue, security practitioners and technology companies will have to pull together to address the challenge. This would involve both better security measures and better information sharing.

Eisen: The first step is to recognize that fraud detection is an inherently moving target. While this may seem obvious, its ramifications are profound. For example, when I develop new strategies, I always think two steps ahead — evaluating each approach not just in terms of its ability to address the current situation, but also in terms of its ability to withstand (or easily adapt to) the fraudsters' next move.

Given the speed by which computer viruses spread, one should ask — how will my bank fare if someone launched a fraud virus or other large-scale fraud attack against my institution?

Katz: You bring up a very important subtlety. The recognition that fraud is inherently a moving target has ramifications not only for strategy development, but also for all aspects of planning, organizing, and equipping the security group. Given the speed by which computer viruses spread, one should ask — how will my bank fare if someone launched a fraud virus or other large-scale fraud attack against my institution? How quickly will my bank become aware of the problem? How rapidly will I be able to identify and block affected accounts?

We found that an effective approach is to think of fraud detection as a risk management ecosystem

Asking these questions may reveal significant weaknesses in current systems. In many banks, fraud detection systems are isolated and rigid. Years of departmental — level acquisitions and single — transaction orientation have resulted in technologies that deal poorly with large-scale attacks. We found that an effective approach is to think of fraud detection (and risk monitoring in general) as a risk management ecosystem where transactions are monitored across channels, findings are shared between detection systems, and the strategy of each system continuously adapt to the situation. Using the topic at hand as an example, if the Internet monitoring system discovers a suspicious Internet session, the information suspected to be compromised during the session is communicated to the check-fraud detection system, which changes the tests it conducts on checks from these accounts.

Eisen: I believe that protecting reputation and trust are the most significant reasons for ensuring a safe banking environment. Of course the ultimate impact of loss of trust is when the customer decides to pick up and move to your competitor across the street. But even before that, if customers start to distrust the email or online channels, customers will revert to using branches or call centers. So protecting the email/online channel has hard dollar impact to the cost of doing business.

For further information, visit www.unisys.com

Specifications are subject to change without notice.

Printed in U S America 8/04

4136 5354-000