Advanced Fraud Solutions

The Rise in Mobile Banking and the Fraud That Comes with It

Five Steps to Help Protect Your Institution from Remote Capture Fraud

What the explosion in mobile e-commerce means for your financial institution and five steps to prevent mobile banking fraud.

GSMA is the leading industry association representing the interests of mobile operators worldwide. Their most recent Mobile Economy 2016 research paper[1] revealed staggering numbers for mobility adoption and penetration:

- By the year 2019 there will be 5.6 billion mobile subscribers
- 5.6 billion subscribers will constitute 70 percent of the world's population in 2019
- By 2020 mobile broadband will account for 92 percent of the world's connections

Enterprise software vendors have been diligently preparing for the onslaught of mobile transaction data that is coming down the pike. And we are already seeing the effects of wide-scale mobility adoption from a shift in consumer banking practices; we are moving from standing in line in the lobby to processing our deposits, withdrawals, and payments online. Initially, this shift occurred on desktops and laptops but as the mobile device continues to serve as portable computer, mobile banking is exploding.

How impactful is the effect of mobile transaction volume to the tech industry? IBM, the most prominent tech vendor on the planet with roots dating back to the early 1900s, recently launched a mainframe built specifically to handle the transaction volume mobile devices will bring to the market in

1. http://www.gsma.com/mobileeconomy/

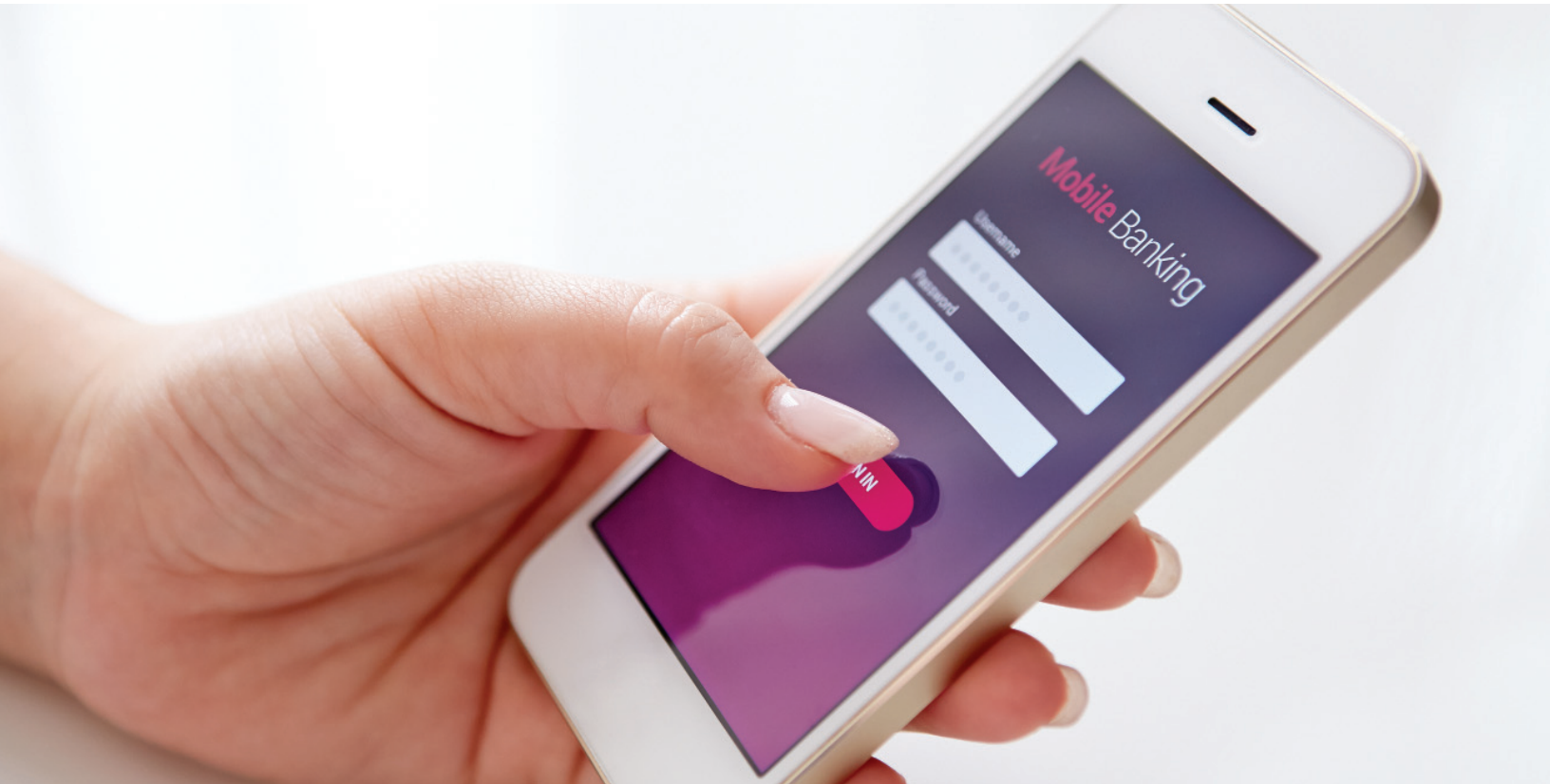
the next five years. A recent Computerworld article reports that the z13 can handle 2.3 billion transactions per day and that "IBM's new z13 mainframe eats mobile app data for lunch."

Over the next five years, consumer banking will undergo a mobile banking transformation to deal with this explosion of mobile banking and mobile e-commerce transactions. Financial institutions equipped to deal with the mobile volume and increase in fraud associated with it, will fare the best.

> "Mobile Banking Has Changed the Way Financial Institutions Work and They are Unprepared for the Onslaught".

A recent survey by research analyst firm IDC found that 64 percent of mobile end users accessed mobile banking solutions from their financial institution (FI). Of that 64 percent, 70 percent were highly active, checking their bank accounts multiple times per week. Not surprisingly, 31 percent of these users check their bank accounts at least once per day. It is clear that mobile banking has arrived; the question is, how well equipped are banks to provide a favorable mobile experience for their customers, without compromising risk and failing on compliance mandates?

Along with this rise in mobile transactions, comes the need for FIs to change the way they work. The ubiquity of mobile deposits has introduced another dimension for fraud detection and compliance. With exponentially more transactions coming in, yet the same number of analysts to audit transactions for fraud, FIs are spread thin. In smaller FIs,



fraud analyst resources are often part-time, splitting duties between mobile fraud and credit-card fraud.

Undoubtedly, mobile banking is putting a strain on fraud prevention as FIs are having to check significantly more transactions, with the same or fewer resources.

Local/Regional FIs Must Automate to Survive

There are options for managing the transaction volume – better process and technology with automation – but few solutions come at a price point that doesn't strain the IT and HR budgets of a local or regional FI. We will look at solutions options later in this paper. The point to make here is that mobile banking has added stress to the workflows of Small/Medium Business (SMB)-sized FIs, and mobile bank fraud is on the rise.

> "Fighting Back with Better Process, Technology and Most Importantly, Automation."

Adding to this burden are regulatory requirements on availability of funds. The Expedited Funds Availability Act (EFAA) of 1987, was legislated long before the smartphone, at a time when deposits came less frequently, and were made in person at the financial institution. Despite the vast changes in consumer behavior over the last 30 years, FIs still are required to make funds available upon deposit, and if there is a need to delay availability "for a reasonable time period," the institution has the burden of proving this reasonably. The door today is wide open for mobile deposit fraud, and the numbers say it's exploding.

A recent survey[2] from a leading research analyst firm found that of the firm's 400 customers, 72 percent identified instances of fraud from remote deposit capture and

2. http://www.prnewswire.com/news-releases/guardian-analytics-releases-mobile-banking-fraud-trends-research-300245222.html

the use of fraudulent checks. The scam is simple enough: 1) The remote deposit is made via mobile device in the parking lot of the bank, then 2) that same check is walked into the bank and cashed as the funds are immediately available but the check hasn't cleared.

Remote capture fraud is exploding across all FIs and the American Bankers Association has reported that 100 percent of recently-surveyed FIs observed remote capture fraud, and its prevalence is up 400 percent across the years 2014 and 2015[3]. Consequently, FIs can't adequately manage all remote capture fraud coming through the pipe, they just aren't resourced enough. Without the bandwidth to audit everything, nor a reliable comprehensive database of fraud information to validate checks, only the higher-amount checks are given the attention to fraud detail, and the losses for SMB FIs are mounting.

Auditing and Compliance initiatives, IT sprawl and service demands from the business side in every enterprise are creating a staggering amount of complexity for banking IT resources to manage. For years now, IT staff have been "all hands on deck" just to manage business service delivery. Strategic research firms such as Gartner, Forrester Research and IDC proselytize about better alignment between CxOs and CIOs, and moving away from the traditional way of thinking that the business side is strategic and the IT side is tactical. In such a world where the IT and Business sides of the enterprise are incentivized to reach common organizational goals, better solutions are created and in theory, the organization is optimized.

Business and industry seem to have come around to the thinking. A result from the closer alignment between the business and IT sides of the workforce comes a higher level of business process aided by technology solutions designed around workflows. With fewer resources to manage the work, relief is provided in the form of better ways of completing the work with technology that provides visibility and automation. Automation is arguably the hottest IT topic today and is what you will find on all meeting agendas between Gartner, Forrester Research, IDC and their respective research clients.

3. http://www.aba.com/Products/Surveys/Pages/2015DepositAccount.aspx

Automation however is not so easily attained at SMB-level FIs. Local/regional FIs don't have the budgets to hire the resources and invest in the technology to be as automated as their enterprise counterparts. Given the increase in volume from mobile deposits and other mobile service requests, local/regional FIs are behind the eight ball. Many times, an un-automated and tactical decision is made to only audit remote deposit captures at amounts of $1,000 and higher. But what about lesser amounts that undoubtedly are adding up?

Some local/regional FIs are turning to vendors like Advanced Fraud Solutions who service this market with automation technology (TrueChecks) that helps mitigate the FI's exposure with notifications of suspicious activity in real time. The secret is a "smart" database that provides a threat-level scoring system to monitor the behavior on each account and then identifies which accounts are at risk. When a transaction comes through with an account number that matches a risky account in the database, the FI is notified and the institution is allowed to investigate and place the account on hold in the meantime.

Pioneers in leveraging data for remote capture fraud, AFS has been working with leading FIs for more than 10 years. AFS has access to the most comprehensive database with which to match fraudulent accounts against, totaling a staggering 7 million records, and the list today continues to grow.

In the anti-virus software industry, global enterprise vendor Symantec provides customers with The Global Intelligence Network, a big-data store of threat "footprints" that they scan perceived threats against and if there is a match, they take a number of automated actions, including "exploding" the virus in a sandbox, just in case. After exposing the threat, they collect the virus' threat indicators (data and meta-data), then adds them to the database. It's impressive technology and solely proprietary.

Symantec and their peers in A/V and end-point security management are not interested in partnering with other providers and herein lies one of the barriers to fighting all cyber-crime across the globe. The fact that AFS is partnering for threat intelligence is a huge positive for local and regional FIs. The data is comprehensive; the product easy to use (you don't have to be an IT resource to use the UI); and TrueChecks, along with other AFS solutions, is sold at a price point that fits the SMB budget. For more information on TrueChecks and other automation-rich fraud-prevention technologies from AFS, please visit www.advancedfraudsolutions.com.

Advanced Fraud Solutions offers a free trial of its TrueChecks product. For more information on taking TrueChecks for a test drive, please visit our website.

Advanced Fraud Solutions

And now, on to the five steps...

Deliver the Fatal Blow to Mobile Check Fraud with These Five Steps

The average time to discover a cyber-breach in 2015 was 201 days.[4] During the Target breach of 2013, it is alleged that a systems admin identified anomalous behavior on the network just a few hours into the breach. Several weeks and millions of compromised credit cards later, the breach was finally discovered and the global retailer started making headlines. The Anthem breach is said to have gone on for nine months before the intrusion was discovered. Remote capture fraud is time-based. Before the FI detects the fraudulent activity, the criminal could have replicated the crime at several other FIs in the vicinity. As with the Target, Anthem and many of the other high-profile breaches, time was not on the side of the organization.

1 Real-time visibility is the key to stem the bleeding.

Clearly, we have a visibility problem in cyber-crime prevention and when the floodgate starts, we don't see the warning signs fast enough to stem the bleeding.

People, process and technology that provides visibility is the key to lowering fraud risk. However, the right people, paired with good workflows (that adhere to compliance standards) and technology is easy to write about, but putting it into practice is another story. Check fraud, computer-virus intrusion, cyber-breach, denial of service — these are the perils of doing business while holding valuable intellectual property. Unfortunately, these attacks will probably never be avoidable, but if you have the proper people, process and technology in place to give you the visibility to get an immediate jump on remediation, you will be ahead of most in the Financial Services industry.

> *"Most people are starting to realize that there are only two different types of companies in the world; those that have been breached and know it and those that have been breached and don't know it."*
>
> — Ted Schlein, Venture Capitalist

4. 2016 Cost of Data Breach Study, Ponemon Institute, www.ponemon.org.

Have accurate, current data with real-time updates to your remote capture system.

There can be no fraud visibility without data. Data is your closest ally. AFS provides client access to one of the most comprehensive remote capture fraud databases in the country. Up-to-the minute data updates provide a real-time and clear picture of whether the account has a history of fraudulent activity at the time of the mobile transaction. Providing visibility with accurate, real-time data from historical transactions removes any fuzziness about the validity of the mobile deposit. The system you use must be able to provide a real-time data feed that includes counterfeit, NSF, Closed Account, Duplicate and other fraudulent items.

Have a real-time alerting system in place that can validate an exception hold.

Accurate, real-time visibility on the probability of a fraudulent remote capture provides the intelligence needed to validate an exception hold. Having the data in your remote capture system is a great start but you need an alerting system that reinforces the reason your institution puts a hold on a deposit. As we saw earlier, we spend most of our working lifetime being overwhelmed in environments where we are asked to do more with less.

It's a constant battle to manage the volume of work while maintaining compliance and industry standards. It's a tremendous help to have alerts to keep your fraud team on task and within the boundaries of compliance. Alerts are a key component of catching fraudulent items at the front line before they become a liability for your institution.

Be sure your real-time alerting system comes with data aggregation and automation.

Real-time alerts for your fraud team starts with work-flow automation. But you must first implement a system that consolidates data from multiple mobile-deposit capture and check image processing platforms. Data aggregation with fraud visibility provides a mechanism for your fraud team to detect, in real time, the validity of a mobile deposit. Upon scan or mobile imaging, the account information is stripped from the check and run against the database. Any anomaly detected during check processing will send an alert to the fraud team, reducing the risk for the FI.

Take a proactive stand against mobile deposit fraud with better data and visibility.

Data quality should be at the heart of your remote capture fraud system if you are

going to minimize remote capture fraud. The mobile scammer who is trying to stay a step ahead of your fraud team is hitting multiple FIs in a single morning or afternoon. Most FIs do not have a full understanding of the remote deposit risk because they don't have the data to give them the visibility to see the magnitude of the problem, resulting in an inability to fight what they cannot see. Real-time updates to your backend database with alerting functions for your fraud team are a critical function to taking a proactive stand against remote capture fraud.

In aggregating the most up-to-date information on the status of the mobile deposit in question, the FI is taking an active position against the risk, rather than reacting to another fraud incident.

In Conclusion

The mobile generation is here. Today there are young twenty-somethings that have only existed in a world of mobility. This generation lives connected 24/7/365, a hand-held computer at their fingertips. Every transaction from good-morning texts to creating photo albums to film making to bank deposits and paying bills takes place on their mobile devices.

As we saw in the survey data from research firm IDC, a large percentage of mobile users check their banking balances multiple times per day. Mobile banking is the new norm and though it makes many things in our daily lives simpler, for FIs the new norm is becoming difficult to manage. It takes the right team with good work processes and viable technology to minimize remote capture fraud and other mobile-generated bank fraud. Remote capture fraud doesn't have to be overwhelming for your fraud team. All you need is consolidation of data feeding your remote capture system, and a process that lends itself to being proactive with mobile check deposit fraud.

There are many solutions on the market for FIs of all sizes. The best fit for you depends on your requirements and how well the solution addresses those requirements now and as your business grows. If you would like a product demonstration from Advanced Fraud Solutions, please contact us at www.advancedfraudsolutions.com.

We would be honored to discuss your business objectives and how we can design a solution to meet your needs.

Advanced Fraud Solutions

1-866-663-4709
www.advancedfraudsolutions.com
info@advancedfraudsolutions.com