ATM FRAUD

An Internal Viewpoint

Lowers Risk Group – Risk Mitigation White Paper Series

LowersRiskGroup™
Protecting People, Brands, and Profits

(540) 338-7151 | www.lowersriskgroup.com

ATM FRAUD

BACKGROUND

Defined as the intentional act of trickery to unlawfully obtain funds from an ATM, most people associate ATM fraud with external crime, where the card or card number and associated PIN are illegally obtained by outside individuals, gangs, or even more sophisticated organized crime syndicates. Considered a form of identity theft by the Federal Trade Commission (FTC), while identity theft had been holding relatively steady for the last few years, the ATMIA *2012 ATM Fraud Report* cites a 45 percent increase in ATM fraud in 2012 alone.[1]

From the onset of the proliferation in the use of ATMs, less sophisticated (but equally effective) methods of ATM fraud include such means as card trapping, skimming, and keypad overlays. Trapping, as the name implies, is where the customer's card is somehow trapped by the perpetrator only to be retrieved later. Skimming is where the perpetrator has put a device over the card slot of an ATM, which reads the magnetic strip as the user unknowingly passes their card through it. These devices require the use of a miniature camera (inconspicuously attached to the ATM) to read the user's PIN at the same time. Lastly, where a hidden camera is not or cannot be employed, a keypad overlay can be used to match up with the buttons of the legitimate keypad below it [pressing them when operated], and records for or transmits to (wirelessly) the perpetrator the keylog of the PIN entries. Collectively, the device(s) illicitly installed on an ATM is/are known as a "skimmer" and the process is known as "skimming".

Today, the criminals have gotten a bit more technologically sophisticated, with the most common types of ATM "cyber fraud" being:

- Cassette Manipulation Fraud - Where the ATM is programmatically altered to dispense multiples of the withdrawal amount with a single cash withdrawal transaction.
- Surcharge Fraud - The programmatic setting of the ATM surcharge to zero on the attackers card.
- Confidentiality Compromise - Where the perpetrator gains unauthorized access to ATM system logs and the confidential information stored therein that can then be exploited.
- Software Compromise Fraud - The catch all for all other ATM fraud that involves the exploitation of software vulnerabilities so as to manipulate the ATM operation itself.

Despite the variety of ways and means that such fraud can be affected, the fact of the matter is that ATM fraud is perpetrated externally, internally, and in some cases by way of some combination of the two. In short, criminals have found that ATM fraud can be committed at lower

[1] Association of Certified Fraud Examiners, 2012 Report To The Nations On Occupational Fraud and Abuse

personal risk, can often be very lucrative, and can usually be carry out without the need for physical force or a weapon.

While the scope of the problem is enormous, as we read/hear about it almost every day in the media, the total cost of ATM fraud in the U.S. is difficult to clearly establish, due in large part to organizations being very guarded about releasing such information as well as the varying forms in which this type of crime can occur.

What we do know is that fraud committed from the inside can be every bit as devastating as external ATM fraud. Fraud committed by the actual person replenishing or servicing the machine can be as simple as pilfering small amounts at a time or more complex with a carefully orchestrated shell game, whereby larger amounts of funds in the machine are siphoned off undetected. In this scenario, the fraudster carefully keeps the residual cash returned to the processing facility in line with the machine dispense totals by sharing (the same or another machine) ATM funds, which goes undetected by those responsible for balancing. A two-person team for dual control, actually performing ATM replenishment, may reduce the opportunity for loss, but may not be practical from a cost standpoint. One ATM servicer alone can have access to over one hundred machines, allowing for an opportunity to steal in excess of a million dollars, undetected for years. These crimes are often times uncovered through mere accident with a fraudster getting out of his or her routine, causing an out-of-balance situation identified at the processing facility and a resulting investigation.

Some fundamental controls that should be in place to mitigate ATM losses include proper registering, issuance and return, inventorying, and storage of access devices, along with completion and accountability of servicing documentation. These fundamental controls are very important; however, they may provide little resistance to the loss in the example above. As an ATM service provider, there are some additional measures that can be implemented to reduce the potential for ATM fraud occurring, or at least from growing out of control:

- Rotate the ATM servicers, so that no one person handles the cash exclusively for a machine over a specified point.
- Develop an ATM cash audit program where the servicer's machines are randomly inspected onsite and balanced by a designated two-person audit team at a specified interval. Greater emphasis and frequency should be with "cash-add" serviced machines.

The latter approach is only as effective as the program implementation. From a practical standpoint, only a small number of the total machines serviced may be audited. However, a significant benefit of deterrence can come from creating awareness with the servicer that any of their machines may be subject to a cash audit at any time.

Preventive measures are typically stifled with cost constraints, particularly where the needs and sense of urgency can be somewhat ambiguous to certain people. However, when a devastating situation unfolds, the need for adequate internal controls becomes quite obvious. While any

preventive approach is an expense, the cost of not doing enough may be far greater in the long run.

THE PLAYERS

ATM Operators

Protecting the cash that funds your ATM program is paramount for every ATM operator. ATM cash differences, thefts, and losses can quickly erode the profitability of an ATM program, or worse, can threaten an ATM operator's ability to continue operations. In recent years there has been a significant increase in cash thefts associated with cash-in-transit (CIT) carriers at their vaults, in transit, and even after the funds have been loaded into the ATM. Some of these losses were covered by insurance, but many found no coverage. In total, these losses have created significant pricing pressure on cash-in-transit insurance which is impacting armored carriers, banks and independent ATM operators alike.

CIT Carriers

The methods CIT carriers use to manage their vault can also have a huge impact on the security and insurability of the cash. Carrier offices with sound operating procedures and security are best positioned to respond quickly and appropriately as issues arise.

These are but a few examples of best practices and they may not be applicable to all carriers. It's understood that not all carriers will be able to follow all of the recommended best practices. In some instances, there may be mitigating circumstances that can help alleviate concerns for customers and cash providers. As banks and independent ATM operators evaluate new and existing CIT carrier relationships a review of their best practices should serve as a guideline.

Insurers

In addition to the cash service vendors and the financial institutions that they serve, insurers face risks either directly from their insured, indirectly when their insured's policy is called upon when the offending vendor's policy is rendered insufficient or invalid due to principal involvement, or when steep competition requires their insured to reduce their premiums and policies to make ends meet.

All this should also provide a similar alert to underwriters. Having the proper guidelines and obtaining answers to relevant questionnaires could enable the insurer to better assess the potential risk. Furthermore, having Lowers & Associates (L&A) conduct cash audits and risk surveys with their insured, will allow for the validating of the questionnaire answers, monitoring of potential risk areas, and create a better foundation for premium reductions based on positive performance. A partnership with L&A makes a winning prospect for all parties involved; lower risk to the insurer, lower losses and premiums for the insured, lower premiums to the insured customers, greater

confidence for the insurer that they have properly calibrated the risk potential of the insured, and greater customer confidence that they have selected the right vendor for outsourcing their cash handling activities.

The Banks

Selecting a quality CIT carrier can be one of the best ways that a bank can minimize the risk inherent in the ATM business as well as to reduce insurance costs. Thorough upfront and ongoing reviews of CIT carriers can help reduce the risk of theft by spotting weak points at the carrier and proactively addressing them. Banks must continually evaluate the due diligence process and continually update their requirements based on patterns of past incidents/thefts and potential means of future losses.

LESSONS FROM ATM LOSS INVESTIGATIONS

Despite the industry stakeholders' best efforts to eliminate or even limit losses relating to ATM theft and fraud, the very nature of the risk makes it ever the more enticing a target of criminal activity. Losses will occur, regardless of the best-laid prevention measures. However, the effect of those losses can be minimized or controlled from a thorough evaluation of each investigation of loss. This truism is perhaps all the more pertinent to internally perpetrated ATM theft or fraud.

First of all, for an ATM investigation to have the desired impact (and for that matter any chance of success), the investigator must be able to determine who had access to the money and when. Where along the money trail was there an opportunity for theft/fraud to occur?

- While stored at the vault?
- During transfer from the vault to the cash preparer?
- From the vault to the cash replenisher?
- While cash was being transported to or from the ATM?
- During cash replenishment?
- During a first-line or second-line service call?
- During ATM balancing or settlement?

All of the above have been some of the traditional avenues of investigation, with the investigator diligently looking for patterns in losses, in ATM access, vulnerabilities, and people. Along the way, the investigator would typically examine how access controls are being enforced (or not enforced) that create opportunities for theft to occur. Perhaps there is a breakdown in dual control at the vault; or maybe unauthorized items are allowed in the cash preparation area that allow cash to be secreted out; or an ATM replenisher is never rotated from a route and begins to set up a Ponzi type of operation; or perhaps unencrypted ATM combinations are left in unsecured servicing

vehicles. In short, there are a myriad of access controls and controls of access devices that can break down along the money trail.

But what if there is no pattern to find? For example, random ATMs mysteriously begin to have large variances during settlement and the cause can't be pinpointed. ATM Servicers claim hardware or software problems; ATM manufacturers claim the thefts are due to the cash vault; the vault personnel blame the ATM cash replenishers; the cash replenishers blame the hardware maintenance personnel. The investigator's job then becomes very difficult, especially if s/he is only looking at the traditional places in the money chain.

Enter the new "wrinkle" in the money chain – a problem that was eventually dubbed "denomination fraud". This fraud/theft targeted almost exclusively "white label" ATMs -- those that are not owned by financial institutions, but instead are owned and installed by private companies around the world.

"Denomination Fraud" occurs when a person accesses the management functions of the ATM and changes the bill denominations to a lower amount than that of the bills actually in the ATM. For example, the bill denominations can electronically be changed to $5 when $20 bills are actually in the ATM. Once the change is made, an ATM user can use a prepaid stored-value card (i.e. with a $500 limit) and request the full amount to be dispensed from the ATM. The ATM (now programmed to believe it has $5 bills in the cassettes, will dispense 100 bills whose real denomination is $20 each. So the ATM user gets $2,000 - a $1,500 "return on investment".

After the denomination fraud is executed, the ATM is changed back to its original configuration so that all appears normal. So how does this happen? For this fraud/theft to be successful, someone has to have the Management Pass Code (MPC) for the ATM. This can come from one of several sources:

- An employee with legitimate access to the code makes the change at the ATM using the ATM's keyboard. Alternatively, s/he can access the ATM remotely and make the change.
- A former employee can do the same if the MPC isn't changed when the employee leaves.
- A current or former employee can give the code to an outsider - someone who won't be recognized if they show up on the CCTV camera at the ATM.
- A person can visit the manufacturer's website where the user manuals for various models of ATMs are posted. These user manuals often conveniently contain the default MPC.

Alternatively, a user can enter the manufacturer's name and ATM model number into a search engine and get the user manual along with the default Master Pass Code from a large variety of sources. Hard to believe, but true.

So, if this type of crime is suspected, where should the investigator look for patterns in losses, access, vulnerabilities, and people? First, was the default ATM Master Pass Code ever changed

by the ATM owner at the time the ATM servicer assumed responsibility for the ATMs? It should have been changed along with all of the ATM combinations.

Second, are the ATMs configured so that remote changes (via telephone or the Internet) to the Master Pass Code can be made, or was this feature disabled? If not disabled, does the ATM owner still have that capability? Get a copy of the ATM set-up parameters for review.

Third, if the Master Pass Code was changed, who at the service company has the Master Pass Code? Where is it stored? Who has access to the storage location and is that access under dual control? Is access documented? Is the storage location under recorded CCTV observation?

Lastly, is the Master Pass Code changed every time a code holder is changed or terminated? Is it changed whenever the MPC is given to a servicer who must use it to reconfigure the ATM? Is it changed after every cash management visit? Are the changes documented? Answers to this set of questions often reveal significant vulnerabilities and are usually a good place to start.

ESSENTIAL CONTROLS

In addition to the best practices identified in the next section, this white paper identifies eight areas where essential controls and loss prevention methods should be made part of the everyday operational fabric of both the CIT and ATM operations. These six areas include (but are not limited to) the following areas:

1. Access Controls
    - ❒ Opening/Closing Procedures
    - ❒ Terminal & Liability Access Devices
    - ❒ General Access Controls
2. Vault
3. Cash Services
4. Transit
5. ATM
    - ❒ General Controls
    - ❒ Traditional Spin Dial Lock ATMs
    - ❒ Non-static Combination ATMs
6. Physical Security
    - ❒ CCTV
    - ❒ Terminal Design
    - ❒ Alarm Systems
    - ❒ Liability Storage

7. Remote Computerized Management of ATMs/ATM Networks
8. Segregation of Administrative Roles

BEST PRACTICES

This white paper presents four essential controls and loss prevention methods that would greatly reduce the likelihood (or at least the impact of) cash service vendor theft, fraud, or misuse of customer funds:

1. Insurance Requirements - Financial Institutions and Insurance policies requiring comprehensive cash/coin and risk/compliance surveys of vendors by third-party auditors on a quarterly basis. Vendors would be required to submit to be eligible for work.
2. External Audits - Financial Institutions and Insurance policies requiring comprehensive cash/coin and risk/compliance surveys of vendors by third-party auditors on a quarterly basis. Vendors would be required to submit to be eligible for work.
3. Standard Audit Framework - The creation of a common set of standards, or auditing body, will allow for comprehensive and unified audits. With all parties participating in one body, directed by Lowers & Associates (L&A), audits performed and results shared would be standardized, comprehensive, and more efficient, and limit vendors to only four audits per year versus multiple individual audits from each of their customers.
4. Vendor Certification - The certification of cash service vendors that prescribes to more rigorous audit and best practice standards would help identify them as low risk business partners with which their customers and insurers can feel more comfortable working.

The need for the financial services industry as a whole to embrace and apply universal fundamental cash handling standards is imperative. Financial institutions doing business with the various vendors should be able to have confidence that these standards are being followed. There should be absolute transparency with the vendors, so the financial institution can see that the appropriate controls are in place and consistently followed, as well as have the ability to have a full audit of all customer inventories, not just their own, whenever requested.

L&A, with its extensive years and expertise in the cash handling industry, knows and understands the "best practices" used today. As stated, L&A has various programs with the leading CIT carriers and insurers to both conduct surveys to evaluate internal controls compliance, as well as perform full inventory cash and coin audits.

CASE STUDY #1: A Domino Effect

The economic consequences to related businesses and insurers go far beyond the simple direct loss of funds, but stretch out like tentacles impinging on the competitive environment and risk further fraudulent activity and losses by other vendors. Case in point, it is believed that in a recent fraud the vendor pursued their fraud to shore up their own business. As the vendor continued to lose money, more money was taken from customer accounts. Because the vendor could not afford to lose customers which would have rapidly accelerated the detection of its fraud, the vendor appeared to have kept pricing to customers extremely low (so low that it may have been unprofitable), thus artificially driving down pricing in the market, preventing competing businesses from capturing their market share, and also weakening competitors who had to follow the vendor's pricing lead to keep their own customers. In this case, it appears that the vendor's fraud was supposedly enacted due to losses from their business line. If competitors are also forced into a loss position then the probability of like fraud occurring there also increases, creating a domino effect. While competition is healthy, illegal competition is destructive.

Conclusion:

In recent years there has been a significant increase in cash thefts associated with CIT carriers at their vaults, in-transit, and even after the funds have been loaded into the ATM. In 2010 alone, there were numerous transit losses including: a high-profile theft where a carrier's owner stole tens of millions of dollars from their own vault, a bold robbery of a carrier vault which resulted in a loss of millions, and numerous bill denomination frauds netting hundreds of thousands of dollars that may have been prevented by the carrier using stronger processes while servicing the ATMs.

"We are in an economic climate where we must remain vigilant," said Mark Lowers, President/CEO of Lowers Risk Group. "Without meaningful security provisions and an ongoing commitment to adhere to them, the exposure to incidents of theft, fraud, embezzlement, etc., remains for the CIT industry. The alternative is increased outside regulatory scrutiny and the potential for more frequent and severe loss experience, something that the CIT industry simply cannot continue to sustain. Implementation of these best practices will add a major hedge of protection around both the ATM and CIT industries."

LOWERS RISK GROUP – Fidelity & Crime White Papers

There are three conditions that are present when fraud occurs: Opportunity, Incentive, and Rationalization. The information contained in these papers demonstrates examples of vulnerabilities and how applying essential controls can significantly reduce the risk of fraud.

ABOUT LOWERS RISK GROUP

Lowers Risk Group combines the services of three industry-leading companies – Lowers & Associates, Proforma Screening Solutions, and Wholesale Screening Solutions – to create a complete risk management service offering for organizations of all shapes and sizes. Employed in concert or on a standalone basis, we excel in providing comprehensive enterprise risk management and human capital risk solutions to organizations operating in high-risk, highly-regulated environments. Our specialized background screening and crime and fidelity risk mitigation services protect people, brands, and profits from avoidable loss and harm. With Lowers Risk Group you can expect an experienced and professional approach to your risk assessment, compliance, human capital, and risk mitigation needs to help move your organization forward with confidence.

Contact Information:

Lowers Risk Group
125 East Hirst Road
Suite 3C
Purcellville, VA 2 0132

Telephone: 540-338-7151
Fax: 540-338-3131
Email: info@lowersrisk.com
Web: www. lowersrisk.com