The Daunting Cost of EMV Upgrades for IADs Solved

The United States ranked number one for losses associated with skimming fraud in the first half of 2011. In 2013, the U.S. accounted for 51 percent of global payment card fraud, according to the Nilson Report.

The U.S. is a more tempting target for ATM fraud like skimming because it has more ATMs than any other country… and because it is not EMV-compliant, according to a paper produced by ACCA USA.

"ATM skimming is a global threat with low risk and high profit for criminals," says David Tente, ATM Industry Association (ATMIA) U.S. executive director.

Experts agree that until the U.S. is fully migrated to EMV, we will continue to see fraud increase.

"Cards without EMV chip technology are easily cloned and can still be used in countries like the U.S., Ghana, Costa Rica, Mexico and Malta that are not fully EMV-compliant," says Tente.

"The number of ATMs in the U.S. – approximately 425,000 – makes it a prime target for fraud," he says.

The U.S. Secret Service reports the average cost of an ATM skimming incident is now $50,000. While most businesses cannot afford to take the chance of losing $50,000, no business can afford to lose the trust of its customers … the real cost of rampant fraud.

EMV Upgrades & Fraud

One of the best steps toward reducing fraud risks is to upgrade ATMs to EMV technology.

In addition to eliminating the risk of having to pay counterfeit card fraud claims, EMV will help to reduce fraud at ATMs and POS, based upon the experience in other world markets. On October 1, 2016, ATM owners and operators will face the daunting possibility of taking on the brunt of any costs incurred through fraud using counterfeited/cloned MasterCard branded cards at their ATMs…unless those ATMs are fully upgraded to be EMV compliant.

According to Bruce Renard, National ATM Council (NAC) executive director, EMV chip technology is far more secure than magnetic stripe when it comes to preventing counterfeit card fraud, and is more difficult with respect to skimming. However, until magnetic stripe technology is completely phased out, it will continue to be an attractive target for criminals to commit fraud at ATMs.

To continue to not be liable for card fraud at ATMs, ATM providers will need to upgrade or replace their equipment to make it EMV compliant. Once EMV compliant, counterfeit card fraud at the ATM becomes of much less risk, says Renard.

"EMV upgrade kits for off-premise ATMs are $200-$300 and up," says Renard. "But that does not include the technician's labor, nor any software costs, installation or testing that may be required."

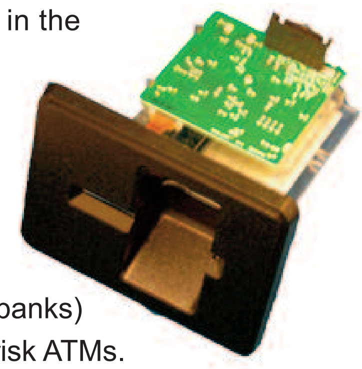
Overall the upgrade costs could run $2,000 to $4,000 per ATM according to estimates from Aite Group. In the off-premise space that's comparable to a new machine. It is no wonder many IADs are wondering if they should simply throw in the towel.

"You don't want to be the last one to upgrade," said James Phillips, Triton vice president of sales and marketing. "As countries around the world migrated to EMV, we saw fraud skyrocket at non-EMV machines in those countries."

"ATMs in major cities with international airports and delivery ports may be at more significant risk in these early stages. But you should not shrug off the fraud risk just because you are inland or have few ATMs," warns Phillips. "Fraudsters are not going to simply close up shop because ATMs in metropolitan areas begin getting EMV card readers installed on them.

They will begin branching out, and with so many smart phone apps out there that can help anyone

pinpoint an ATM anywhere in the U.S., it won't be hard for them to find at-risk ATMs."



"The other risk for ATM owner/operators is that the parties further up the food chain (processors, sponsor banks) decide to simply shutoff at-risk ATMs.

As Canada migrated to EMV we saw small areas, with very few ATMs, began seeing so much fraudulent traffic that processors shut down those machines until they were upgraded," notes Phillips.

How to Upgrade & Stay in Business

ATM deployers don't need to weigh the cost of upgrading their terminals to EMV versus taking on liability for unnecessary fraud costs. There are options says, Darrin Ginsberg, CEO of Super G Funding, a top residual lending company and trusted partner among ISOs, ATM deployers and merchant services.

As IADs begin making plans to upgrade their terminals and looking at their balance sheets, Ginsberg and his team offer some advice.

⏩Bank Loans

A traditional bank loan, a SBA loan or a home equity loan against their home are options.

Traditional loans pose challenges. One of the biggest is the current tight credit market for small businesses. While there has been significant talk of economic recovery in the U.S., that relief has not yet spread to the small business sector.

"Another factor for IADs is that financial institutions simply don't understand the business model," says Jon Engleking, Super G COO. "Banks typically have strict credit criteria based on eligible collateral and residual streams from ATMs are not traditionally considered an asset."

"Banks also have to know how IAD residual streams evolve in order to properly manage that risk – something institutions are unlikely to look into unless they are focused on lending to payment processing-based businesses," Engleking continues.

Selling Off Part of Your Portfolio

Some IADs may be tempted to sell off a portion of their portfolio to raise funds for EMV upgrades.

Engleking advised IADs not to sell. "You should really avoid selling any part of your portfolio until you want to leave the business."

Proceeds from a sale are taxable income, Engleking notes, and a smaller portfolio means less income moving forward. Despite the initial increase in cash, those selling off pieces of their business are looking at a pretty big long term loss.

Taking on Investors

An infusion of cash from an investor is another option. Equity investors allow a business to sell shares of the company to investors without the risk of debt.

"Equity investors share in your upside and may require giving up control of your business and require approval for the expenditure of funds. They also have the potential to create a conflict as to the timing of and terms of the sale of your business. Equity partners may force you to try and grow too quickly without having time to learn certain lessons that come with any new business. Equity investors are permanent unlike lenders who are gone once repaid," says Ginsberg.

Borrowing Against Residuals

A new alternative — borrowing against residuals — has recently been offered to the ATM industry.

A residual loan allows an IAD to borrow against their monthly income, which is not typically recognized as an asset by banks, rather than the value of their ATM hardware.

Working with the processor, the loan is paid back through a monthly draw-down for interest and principal before the borrowing IAD receives the residuals, typically the next business day.

Super G Funding, allows IADs to borrow against their residuals and is able to offer more credit availability — $25,000 to $5 million — with longer term structures than any other financing source.

And, because Super G understands the ATM business model, there are no hoops to jump through like with a bank, the application process is simple and loans can be closed in as little as seven business days.

"Since a residual loan's criteria is based on an IAD's recurring revenue, personal credit history is not as big of a factor than with a traditional bank loan," says Super G Vice President of Business Development Bob Sliker. "Instead, residuals lenders look at the past 12 months of residuals, what makes up the residual stream, how those residuals are performing and base the risk factor on those criteria."

In addition, funds are available in installments — giving IADs time to upgrade a portion of their fleet before taking another installment, notes Sliker.

No matter how you plan to pay for EMV compliance, it is important that you protect your business from unnecessary costs associated with fraud. IADs have funding options — there is no need to weigh the cost of fraud liability versus the cost of upgrading your terminals.