

White Paper

Branch ATM Network Isolation: Reducing Network Vulnerability and PCI Audit Scope

Introduction

Automated Teller Machines (ATMs) are vital to a financial institution's (FI) service delivery and marketing communications. According to the World Bank, there are close to 3.5 million ATMs in use worldwide.¹ Billions of transactions are carried out and processed every day with the help of ATMs, making them a key staple of the Omnichannel banking experience today's customers have come to expect.

Given the sensitivity of the data they transact, it is critical for ATMs to have a secure network connection. Traditionally, FIs have relied on the existing branch network to connect ATMs to financial payment gateways or processors. This was, historically, cost-effective and easy to do.

However, changes to industry requirements in recent years have made this implementation harder to navigate. This is because networks in which ATMs share connectivity with other systems and devices create vulnerabilities for the Cardholder Data Environment (CDE). Thus, they are not deployed without extensive work, costs, and compensating controls. Payment Card Industry (PCI) standards, developed and mandated by the major credit card brands, have established requirements that further complicate matters and can be difficult to interpret, implement, and uphold.

In order to overcome these challenges, a growing number of banks and credit unions are isolating the ATM or CDE on a standalone, PCI-compliant network. By doing so, they greatly reduce cardholder risk and ensure sensitive data only traverses pathways designed to handle it. ATM network isolation allows FIs to deploy ATMs and CDE devices on a separate, completely isolated network. This means no shared connectivity with anything on the branch network. Furthermore, due to the popularity and capabilities of Managed Network Services Providers (MNSP), many banks and credit unions are enlisting third-party vendors to handle the entire ATM isolation implementation including deployment, monitoring, and lifecycle management.



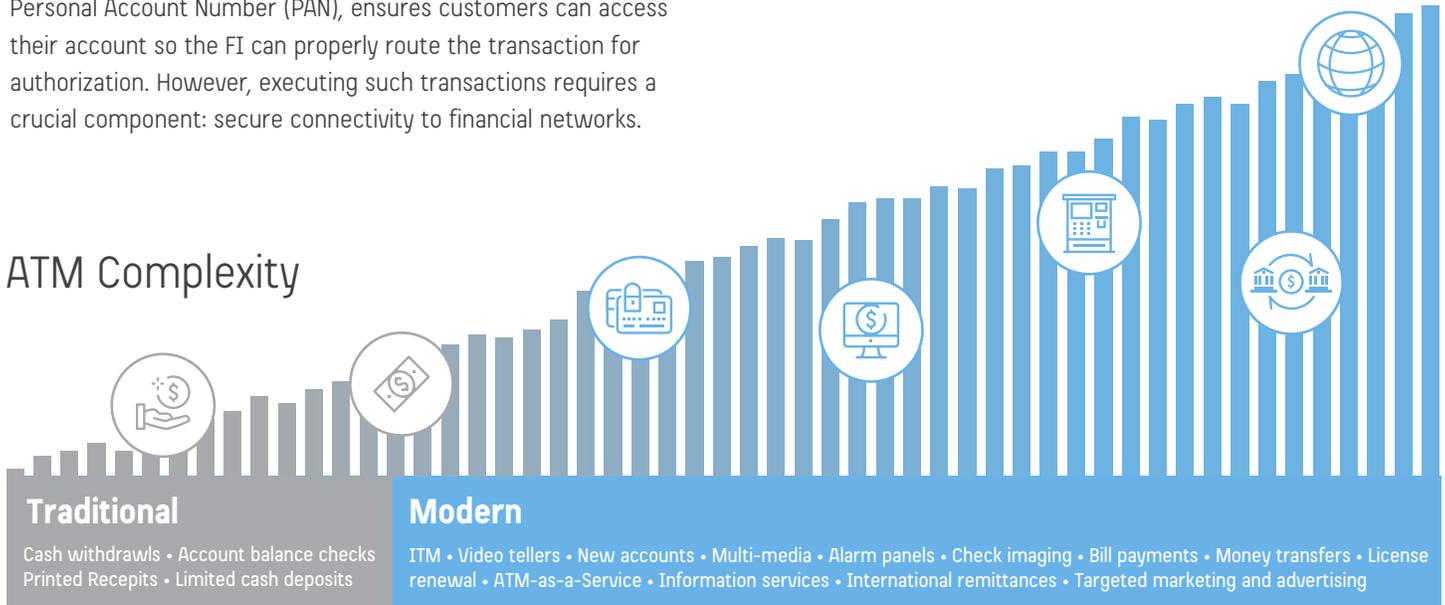
— 3.5 million —
ATMs currently in use worldwide

**ATMs are handling
more types of
transactions than
ever before**

The ATM in Omnichannel Banking

The increasing popularity of web-based banking and mobile applications has helped establish the ATM as a "physical bank" for today's consumer. In order to accommodate every customer, FIs deploy ATMs at various locations including branch and remote sites. The standard ATM debit/credit card, with a 16-digit Personal Account Number (PAN), ensures customers can access their account so the FI can properly route the transaction for authorization. However, executing such transactions requires a crucial component: secure connectivity to financial networks.

ATM Complexity



The pervasiveness of hacking, viruses, and malware has led to scrutiny around network decision-making. Furthermore, skimmers, pinhole cameras, and other devices used to illegally capture PIN entry and other customer data are now more common than ever. Modern branches bring a whole new array of devices and emerging technologies that introduce risk such as digital display signs, Wi-Fi for both corporate and customer use, tablets used by bankers, self-service kiosks, and other similarly connected devices. Many of these devices share connectivity and may expose the network and its components to vulnerability.

Since theft, fraud, and hacking can come from inside the network, it is critical for FIs to protect transactions from internal vectors as well. Tighter security controls now exist for ATMs; software has improved and anti-virus/anti-malware protection has become standard. While such controls help protect the ATM, they are not 100% effective against all attacks. ATMs on the branch network render the entire branch, and possibly the entire organization, in-scope for PCI auditing.

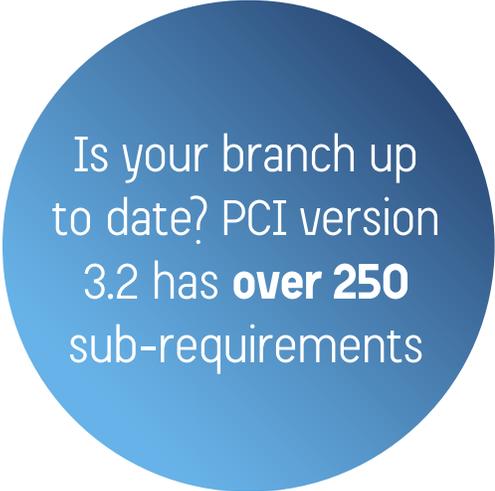
Without adequate segmentation, the entire network is in-scope for PCI auditing.

PCI and Why it is Important

The PCI Data Security Standard was developed by the founding payment brands of the PCI Security Standards Council, including VISA, American Express, Discover Financial Services, JCB International, and MasterCard, to help facilitate broad adoption of consistent global data security measures.² Such measures are vital for ATM operators to understand given the sensitive card data ATMs process.

For better or worse, most payment systems are still tied to the 16-digit PAN. Indeed, the PCI standard was established in part to protect the security and integrity of this number. The nature of payments, and structure of our financial systems, means that this format is unlikely to change any time soon.

PCI version 3.2, released in April 2016, contains over 250 sub-requirements.³ These guidelines can be complicated to understand and even more difficult for a bank or credit union to implement. On top of that, security controls and protocols must be regularly tested to ensure continual compliance with the standard.



Is your branch up to date? PCI version 3.2 has **over 250** sub-requirements

The Consequences of a PCI Breach

The cost of a PCI-related breach can be substantial. In recent years, both Target and Home Depot were victims of highly publicized breaches. With Target, attackers were able to gain entry via an HVAC system connected to the network and steal cardholder data from a database, affecting more than 40 million customers.⁴⁵ The company spent over \$200 million on legal and settlement costs related to the breach.⁶⁷ However, this number does not account for the indirect losses in sales and revenue associated with declining consumer confidence and reputational damage. The Home Depot breach was similarly devastating, affecting over 50 million customers and costing the company nearly \$200 million.⁸⁹

A bank or credit union affected by a major PCI-related breach would potentially have to reissue their entire card base to avoid facing legal action from consumers or partner institutions for failing to protect cardholder data.

In the case of a mass reissue, even just the card plastic will be expensive since an EMV chip must be embedded and programmed. Beyond that, customers need to be notified, and the shift in confidence will likely result in accounts being closed, creating a permanent loss for the bank or credit union. In addition, payment brands such as VISA and MasterCard, which have their own reputations to safeguard, have authority to pull their agreements from non-compliant FIs.

PCI-related breaches can cost millions

The Role of the PCI Audit

PCI audits can be triggered in a variety of ways. Most FIs have an independent internal audit department which typically reports directly to the board or a supervisory committee. Independent accountability helps ensure the department can effectively assess and understand the institution's risk appetite, and report findings to management. The scope of internal auditing within an organization is broad and includes compliance with laws and regulations. The internal audit department may determine that proactive self-inspection of PCI compliance is warranted, in part, to work towards and achieve PCI compliance before an outside source requests it. As a result, they can help the organization better manage risk.

Card brands want proper controls in place to protect the integrity of their networks, customers, and brand names. They may require regular reporting on PCI compliance as part of their agreement. This could include a self-assessment questionnaire or a report from an independent, external auditor.

Finally, the FDIC and NCUA, as the primary insurers of banks and credit unions, can enforce adherence to industry norms, compliance standards, applicable laws, and regulatory requirements. Their power is vast: they can shut down FIs deemed to be too high risk for consumers. Additionally, the FDIC or NCUA themselves may require PCI audits during regular assessments of an institution. Often, they will advise in advance that adherence to PCI will be part of the next audit review.¹⁰¹¹¹¹²¹³ These forewarnings are invaluable in affording the FI time to prepare. Specifically, banks and credit unions can determine to what extent they are in compliance, find any gaps, and take preventative steps before the audit, reducing noted exceptions.

Why ATM Network Isolation is the Best Approach

While standard network segmentation is a step in the right direction, the added implementation infrastructure can increase the amount of networking equipment required to support the branch. This includes the necessary dedicated switches and firewalls to regulate the ATM or CDE, containing it from the rest of the branch network. Furthermore, while segmentation does reduce PCI scope on the branch network, it often increases complexity, implementation costs, and internal IT responsibilities.

Undoubtedly, the most comprehensive solution is achievable with an isolated ATM or CDE network. In this configuration, an entirely separate network is deployed - one which does not share connectivity with any branch devices or machines. ATM network isolation offers the kind of physical separation from the branch network that standard segmentation does not provide, and at the same time demands fewer IT resources.

Another benefit to ATM isolation concerns the customer experience. If a flat, interconnected network loses connectivity, every device on that network will lose functionality, negatively affecting customers. In an isolated configuration, even if the main branch network loses connectivity, the ATM can still function. By isolating the ATM to its own network, the FI can ensure customers have access to account services regardless of the branch network's status.

Ensure customers
have access to their
account

Outsourcing Isolation

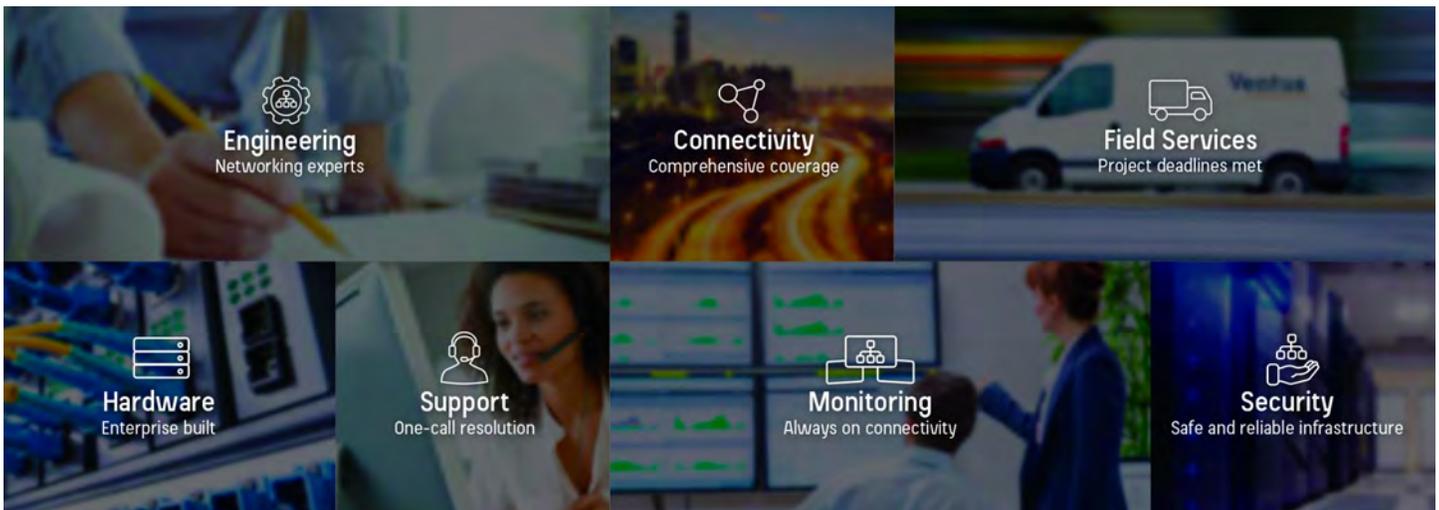
PCI compliance is a requirement for all FIs. However, managing the networking details in order to reduce PCI scope can be complicated and costly. Indeed, many branches have been around since before PCI was even a consideration, and their legacy infrastructure is still deeply entrenched in operations. The ongoing, direct support of networking hardware, connections, and devices requires staff, resources, and time, all of which add to an FI's costs. As a result, banks and credit unions must evaluate how they want to direct efforts and resources toward meeting PCI requirements.

Thankfully, modern Managed Network Services Providers have made offloading or outsourcing CDE network isolation less complicated and more achievable. An increasing number of FIs are using PCI-compliant, 3rd party vendors who can isolate the CDE for them, ensuring compliance and reducing the scope of an audit. This approach frees the institution from the burden of having to troubleshoot the networking details and changes on their own.

The widespread adoption of cellular wireless technology for ATM connectivity has made the transition to CDE isolation even easier. Wireless routers designed specifically for ATMs can be rapidly deployed and installed, getting an isolated network up and running immediately. While cellular has led the way, some scenarios or configurations may require alternate types of connectivity. One example is an ITM network that delivers video traffic via fixed line service and ATM traffic via PCI-compliant cellular.

MNSPs offer a crucial benefit in this regard, possessing the resources and expertise to manage multiple connectivity circuits and associated vendors. This allows the provider to implement the most appropriate network across a diverse ATM environment. With an MNSP managing network isolation, financial institutions can reduce PCI audit scope and focus resources and time on their core business.

Managed Network Services Providers have made network isolation less complicated and more achievable.



Sources

- ¹ "Automated teller machines (ATMs) (per 1000 adults)," The World Bank, retrieved 3 January 2018 from <https://data.worldbank.org/indicator/FB.ATM.TOTL.P5?view=chart>
- ² "About Us," PCI Security Standards Council, retrieved 3 January 2018 from https://www.pcisecuritystandards.org/about_us/
- ³ "Payment Card Industry (PCI) Data Security Standard Requirements and Security Assessment Procedures Version 3.2 April 2016," PCI Security Standards Council, retrieved 3 January 2018 from https://www.pcisecuritystandards.org/documents/PCI_DSS_v3-2.pdf?agreement=true&time=1515605668112
- ⁴ Krebs, Brian. "Target Hackers Broke in Via HVAC Company," Krebs on Security, retrieved 7 November 2017 from <https://krebsonsecurity.com/2014/02/target-hackers-broke-in-via-hvac-company/>
- ⁵ CNNMoney Staff. "Target: 40 million credit cards compromised," CNN Money, retrieved 8 November 2017. <http://money.cnn.com/2013/12/18/news/companies/target-credit-card/index.html>
- ⁶ Abrams, Rachel. "Target to Pay \$18.5 Million to 47 States in Security Breach Settlement," The New York Times, retrieved 8 November 2017 from <https://www.nytimes.com/2017/05/23/business/target-security-breach-settlement.html>
- ⁷ "Target Corporation Annual Report," Unites States Securities and Exchange Commission, retrieved 8 November 2017 from <https://www.sec.gov/Archives/edgar/data/27419/000002741917000008/tgt-20170128x10k.htm>
- ⁸ Roberts, Jeff John. "Home Depot to Pay Banks \$25 Million in Data Breach Settlement," Fortune, retrieved 9 November 2017 from <http://fortune.com/2017/03/09/home-depot-data-breach-banks/>
- ⁹ "Home Depot Settlement Agreement and Release," SCRIBD, retrieved 9 November 2017 from <https://www.scribd.com/document/341431754/Home-Depot>
- ¹⁰ "Who is the FDIC?," Federal Deposit Insurance Corporation, retrieved 14 November 2017 from <https://www.fdic.gov/about/learn/symbol/>
- ¹¹ "2015-2019 Strategic Plan," Federal Deposit Insurance Corporation, retrieved 14 November 2017 from <https://www.fdic.gov/about/strategic/strategic/supervision.html>
- ¹² "Financial Institution Letters," Federal Deposit Insurance Corporation, retrieved 14 November 2017 from <https://www.fdic.gov/news/news/financial/2008/fil08127a.html>
- ¹³ "Approved Corporate CUSO Activities," National Credit Union Administration, retrieved 15 November 2017 from <https://www.ncua.gov/regulation-supervision/Pages/corporate-large/credit-union-service-organizations/approved-activities.aspx>



For more information about Ventus Managed NaaS
please email info@ventusgns.com or call **866.949.9994**