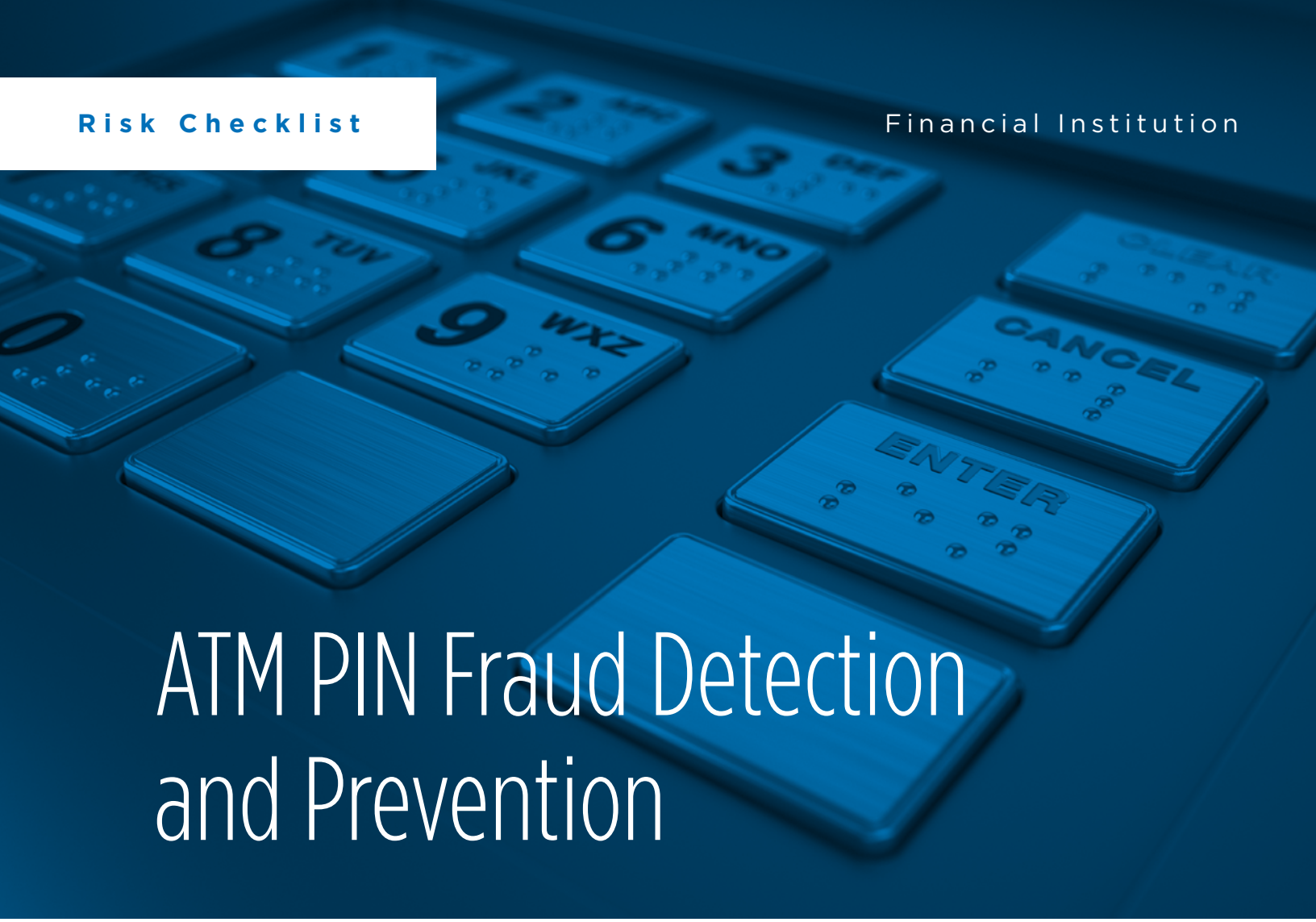
Risk Checklist

Financial Institution



ATM PIN Fraud Detection and Prevention

Many widespread card breaches originate from ATM PIN fraud attacks, which continue to become more sophisticated.

Follow this checklist to better protect your financial institution and consumers from an ATM fraud attack.

Allied Solutions

May 2021

ATM PIN Fraud Detection & Prevention Checklist

- ☐ Add anti-skimming hardware and alerting software to your ATMs, starting with any that have previously been compromised. Contact your ATM vendor for more information on this technology.
- ☐ Install measures for the identification, jamming, or disturbing of skimming devices already attached to an ATM.
- ☐ Have alerts sent to your financial institution when an ATM is tampered with.
- ☐ Install privacy shields to hide consumers' hands as they input PINs.
- ☐ Display warnings about skimming devices and available incident report channels on or near the ATMs.
- ☐ Perform daily inspections of ATMs to help identify any foreign object or skimming device.
- ☐ Watch for any unauthorized wireless cameras in the surrounding area of the ATM.
- ☐ If you use a door for entry into the ATM, inspect the door for a skimming device. Consider removing the card reader and using another type of consumer authentication measure, or leave it unlocked.
- ☐ Use lighting surrounding the ATM to help prevent an attack against a consumer using the ATM.
- ☐ List a telephone number to call if the consumer suspects any fraud attempts at the ATM.
- ☐ Confirm PIN authorizations at your ATMs are going through your Fraud Monitoring System.
- ☐ Immediately block and reissue compromised cards.

Visit our website for more risk education:
alliedsolutions.net/bond

Allied Solutions
GROW, PROTECT AND EVOLVE YOUR BUSINESS.®

ATM PIN Fraud Response & Mitigation Checklist

- ☐ Review the PIN change reports in detail to find out how the PIN change was performed.
- ☐ Validate what type of security is used when the cardholder is requesting a PIN change.
- ☐ Confirm with the cardholder to find out if they requested the PIN change to determine if they may have been "phished" by the card criminal.
- ☐ Confirm whether or not the card with the PIN fraud was on one of the card data breach reports.
- ☐ Contact the ATM hardware and software vendor to find out if malware may have been installed if an increase in unauthorized ATM PIN withdrawals is noted.
- ☐ Review ATM PIN daily dollar limits to see if they have been removed or increased.
- ☐ Review ATM transaction limits to see if they have been removed or increased.
- ☐ Check to see if there are any other system or programming changes taking place on ATM PIN authorizations.
- ☐ Run a special report to analyze the dollar amounts associated with a PIN authorization.

975-R10-5.21