Allied Solutions

Allied INSIGHTS

Fraud & Security RISK ALERTS

Timely insights to protect against fraud and mitigate risks

Emerging "Ghost Tap" Fraud Leveraging Stolen Mobile Devices

SUMMARY

Financial institutions should be aware of a rapidly evolving fraud scheme combining mobile device theft, account takeover, and advanced payment manipulation. Criminal networks are targeting consumers at large public venues (e.g., concerts, festivals, sporting events) to steal smartphones and exploit mobile wallet functionality for fraudulent transactions.

This emerging threat highlights the convergence of physical theft and advanced payment fraud. By exploiting trusted authentication methods such as mobile wallets, criminals are able to conduct fraudulent transactions that may appear legitimate. Proactive controls, enhanced monitoring, and accountholder education are critical to mitigating this evolving risk.

HOW THE SCHEME WORKS

- **Targeting and Theft:** Criminals identify individuals using mobile wallets in crowded environments. The victims' device passcodes are observed or recorded while making purchases or unlocking the device. The device is then stolen.
- **Account Takeover:** Using the passcode, fraudsters quickly reset the device's account credentials (e.g., Apple ID), locking out the account owner. The fraudster then has full access to the mobile wallet and other sensitive applications.
- **Device Trafficking and Monetization:** Stolen devices are often shipped in bulk to organized fraud operations overseas. The devices are maintained in "phone farms" with active digital wallets.
- **"Ghost Tap" (EMV Relay) Fraud:** Fraudsters remotely relay payment credentials from stolen devices to a separate device at a POS terminal. The

transactions appear as legitimate contactless payments and therefore bypass traditional fraud controls.

KEY RISKS TO FINANCIAL INSTITUTIONS

- Increased fraud losses from contactless/mobile wallet transactions.
- Account takeover exposure when devices and passcodes are compromised.
- Difficulty detecting fraud due to legitimate authentication signals.
- Expansion into high-value fraud scenarios, including fuel theft and retail purchases.
- Growing activity in the U.S., following significant increases observed internationally.

BEST PRACTICES

- **Transaction Controls:**
  - Restrict or disable offline transaction approvals, particularly for higher-risk merchant categories.
  - Monitor for anomalies in contactless transaction activity, including velocity and geographic inconsistencies.
- **Authentication and Digital Wallet Security:**
  - Strengthen controls around digital wallet provisioning and authentication.
  - Implement step-up authentication for higher-risk transactions or behavioral anomalies.
- **Fraud Detection and Monitoring:**
  - Enhance monitoring indicators of account takeover linked to mobile device compromise.
  - Identify patterns consistent with EMV Relay (“Ghost Tap”) activity.
- **Card and Payment Strategy:**
  - Continue efforts to reduce reliance on magstripe transactions by only allowing EMV (chip) authentication.
  - Evaluate EMV configuration settings to ensure appropriate validation controls are in place.
- **Accountholder Awareness:**
  - Educate accountholders on safeguarding device passcodes.
  - Encourage use of biometric authentication where available.
  - Promote immediate reporting of lost or stolen devices. Individuals should cancel cards immediately, use “Find My iPhone” to wipe the device, and report the IMEI code to their phone carrier.

RISK MITIGATION RESOURCES

- Visit our NEW Fraud Prevention Center for additional risk resources.
- Learn about the Top 7 AI-Generated Retail Scams.
- Stop scams together with Operation Shamrock.
- Learn how your card readers can combat skimming.
- Read more about Ghost Tap & PhantomCard.

Need assistance or want to request a consultation?

Contact our risk specialists at risk_specialist@alliedsolutions.net

The information presented in this email is intended for informational purposes only and should not be construed as legal advice or a legal opinion and it may not reflect the most current legal developments. You should seek the advice of legal counsel of your choice before acting on any information provided in this email.