VISA SECURITY ALERT JULY 2018

FRAUDSTERS TARGETING CALL CENTER CHAT AND NON-VOICE CHANNELS

DISTRIBUTION: ISSUERS, ACQUIRERS, MERCHANTS AND AGENTS

EXECUTIVE SUMMARY:

A growing industry trend to deploy artificial intelligence (AI) that supports online chat and non-voice channel services within call centers and merchant online environments may introduce potential risks to the users of these services. According to a recent report by PYMNTS.com, 85% of all call center interactions will not require a human employee by 2020. Visa Payment Systems Intelligence (PSI) identified increasing instances of criminals targeting these online services to obtain payment data.

Use of chat and non-voice channels can be an efficient method for managing customer interactions, however, the risk of potential exploitation grows if additional anti-fraud and security measures are not used in conjunction with these services. Without proper vetting, these services and software solutions provided by third-parties potentially introduce the risk of logical errors or vulnerabilities that may be discovered and exploited by criminals. The purpose of this Visa Security Alert is to provide clients with an understanding of the threat landscape and best practices for securing this environment.

Targeting Chat and Non-Voice Channels

AI technology is increasingly important as call centers become the primary customer interaction point for many payment system participants and their clients. Due to the rise in online and mobile commerce, payment system participants and their agents are deploying AI solutions to assist with increasing call volumes. Further, many call centers are also expanding services to help close potential sales. New chatbot and non-voice AI services are used to quickly answer customer questions regarding goods/services and drive users to complete the sale.

Visa is aware of attacks where threat actors compromised online chat service providers and were able to distribute malware to merchant clients designed to intercept payment card data during checkout. Visa assesses that fraudsters will continue to target online chatbot service providers to commit fraud as more consumers rely on this resource to interact with merchants and financial institutions.

Best Practices

Just as with any other vendor, Visa clients and merchants should thoroughly vet any third-parties that provide chat and non-voice channel support for payment acceptance or processing. Clients and merchants must take care when integrating chat solutions to ensure payment data is never exposed or at risk due to these services. If the chat solution is designed to support payment account capture as part of its functionality, the vendor must be PCI DSS compliant and registered as a Visa Service Provider. While some of these third-party service providers may not process payment data, their services still have the ability to introduce risks due to connectivity and integration into both financial institution and merchant web sites.

As with all new technologies, new products should be thoroughly tested and reviewed for vulnerabilities before implementation. Visa recommends a tiered implementation approach as the best defense to include educating contact center staff in addition to the use of new authentication technologies and advanced analytics. Third party service providers should also deploy thorough logging and monitoring defenses to detect unusual system activity. Visa's PSI team will continue to provide further details of the threat actor's tactics, techniques and procedures as more information becomes available.

Visa Global Registry of Service Providers

Agents are important players in the development of acceptance infrastructure, new payment channels, and securing the promise of a trusted payment system. Visa is committed to drive transparency through information sharing and awareness of agent risk profiles.

The Visa Global Registry of Service Providers is Visa's designated source for information on registered and PCI DSS-validated agents that provide payment-related services to Visa clients and merchants. Service providers that store, process or transmit Visa payment data must be registered with Visa and demonstrate PCI DSS compliance.

Please note: As specified in the Visa Rules (ID 0025895), before registering an agent, a Member must complete and validate compliance with the applicable regional due diligence standards. A Member with a registered Third Party Agent must perform an annual review of the Third Party Agent to confirm ongoing compliance with applicable regional due diligence standards.

To report a data breach, contact the Visa Payment Fraud Disruption team:

- Asia Pacific Region, Central Europe/Middle East/Africa Region: VIFraudControl@visa.com
- Europe: Datacompromise@visa.com
- LAC: LACFraudInvestigations@visa.com
- U.S. and Canada: USFraudControl@visa.com