WEBINAR SUMMARY

August 20, 2020

First Contact – Vulnerabilities in Contactless Payments

Leigh-Anne Galloway, Head of Commercia Research, Cyber R&D Lab
Timur Yunusov, Head of Offensive Security Research, Cyber R&D Lab
Karl Klaessig, Director of Product Marketing, Security Operations, ServiceNow

KEY TAKEAWAYS

- It is unclear whether contactless payment has resulted in fraud reduction.
- The process of authenticating contactless payments leaves Visa vulnerable.
- As contactless banking increases, financial organizations are facing security challenges.
- Automation accelerates IT and security response to incidents.

in partnership with

OVERVIEW

Contactless payments are quickly replacing traditional cash and chip-inserted credit card transactions. Despite using a seemingly modern technology, it is still not clear whether near-field communications (NFC) cards and mobile devices are driving a reduction in fraud.

Regardless of the vulnerabilities found in vendor payment cards, banks are still responsible for protecting customers from theft and fraud. Automated solutions can help financial institutions—many of which are still using manual, siloed processes—to increase their capacity to respond to vulnerabilities and incidents and ultimately decrease the size and cost of a breach.

CONTEXT

Leigh-Anne Galloway and Timur Yunusov discussed vulnerabilities in contactless payment card systems, such as Visa. Karl Klaessig shared how automated solutions can help banks respond more quickly to security incidents and help prevent breaches.

KEY TAKEAWAYS

It is unclear whether contactless payment has resulted in fraud reduction.

Adoption and use of contactless credit cards have increased rapidly. But it is still not clear whether payments via near-field communications cards have reduced fraud.

Reports from Visa Europe and the UK's national fraud and cybercrime reporting center, ActionFraud, are conflicting, and the raw data is not available.

Tale of Two Reports: Conflicting Information from Visa Europe and ActionFraud	
Visa Europe	Fraud rates declined by 40% in Europe between 2017 and 2018
ActionFraud	Contactless card thefts doubled in 10 months between April 2017 and January 2018

> It's hard for us to know if contactless has resulted in fraud reduction. But if we look at independent bodies like ActionFraud, it looks like this probably isn't the case.
>
> *Leigh-Anne Galloway, Head of Commercial Research, Cyber R&D Lab*

The process of authenticating contactless payments leaves Visa vulnerable.

Prior to contactless payments, most big-brand credit card companies used a standard way of carrying out transactions. With the introduction of NFC, Mastercard and Visa used similar workflows but different authentication processes, which ultimately leaves Visa vulnerable to theft.

One area of risk arose from Visa's decision to put an emphasis on transaction speed, which resulted in eliminating card authentication and placing more emphasis on online authorization. This opened up the company to greater risk of fraud. Conversely, Mastercard chose to put even more emphasis on offline authentication, making it mandatory for all contactless cards.

Tap and go limits create a second area of risk for Visa cards. When the Visa card sends the application cryptogram (AC) to the terminal, it includes two key transaction qualifiers:

- The card transaction qualifier (CTQ)
- The terminal transaction qualifier (TTQ)

The TTQ includes supported contactless transaction features, while the CTQ includes supported verification methods, such as PIN, signature, or the mobile device's consumer device cardholder verification method (CDVCM).

Tap and go limits	
Soft limit	Set by the country where the transaction occurs: Maximum that can be charged before requiring cardholder verification, such as a PIN or signature. *Example:* If a US Visa card is used in the UK, UK limits apply.
Hard limit	Set by the country where the card is issued: Maximum that can be charged before requiring cardholder verification, such as a PIN or signature. *Example:* Since UK sets its own hard limits, if a UK Visa card is used in the US, UK limits apply.

CDVCM, which was introduced with Apple Pay, often carries limits much higher than either the soft or hard tap and go limits (e.g., £5,500 and US$10,000 compared to a £45 soft limit in the UK today).

Without the TTQ and CTQ information sent in the card's application cryptogram (AC), a criminal conducting credit card fraud can convince the terminal that CDVCM is supported, allowing high-cost transactions to occur without verification.

The Cyber R&D Lab found that all Visa cards and all cryptograms used by these cards were affected, including those issued in the UK, European Union, United States, and Asia. American cards still use chip and signature, which makes it more difficult for attackers to take advantage of this method.

> We found this affects every Visa contactless card; none of the cryptograms at the moment check card transaction qualifiers or terminal transaction qualifiers.
>
> *Timur Yunusov, Head of Offensive Security Research, Cyber R&D Lab*

Banks Own the Cost of the Fraud

Consumers are rarely responsible for fraudulent charges; the issuing or acquiring banks are responsible for returning the money back to the customer when fraud occurs.

These banks are also likely to be on the hook for mitigating the problem.

Cyber R&D Lab provided the vulnerability information to Visa more than 18 months ago but is not seeing Visa taking steps to solve the problem. Instead, the lab is working with banks to ensure they can mitigate the problem.

As contactless banking increases, financial organizations are facing security challenges.

Even before COVID-19 created a more homebound, lower-contact environment, banks were seeing customers moving away from branch banking to online and more recently mobile banking. For instance, a recent Citi Mobile Banking Survey suggests that "91 percent of mobile banking users prefer using their app over going to a physical branch, and 68 percent of millennials who mobile bank see their smartphones replacing their physical wallets." This significant shift, while exciting for consumers, is increasing security challenges for the financial institutions.

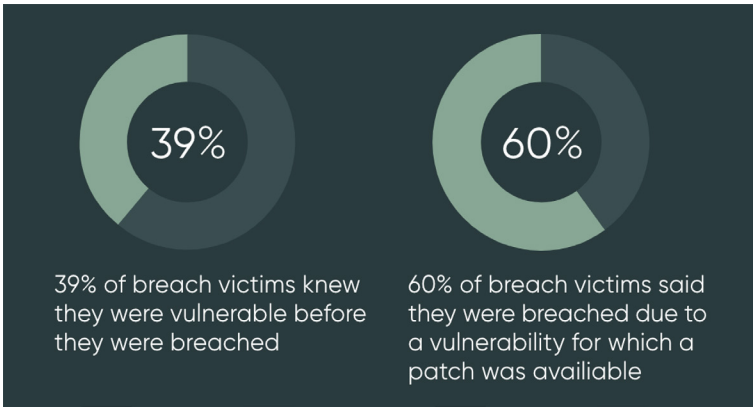
Security teams are finding it increasingly difficult to prioritize incidents quickly. Challenges include:

- **No context.** 76% of organizations have no common view of assets and applications across security and IT.
- **Few resources.** 82% of employers report a lack of cybersecurity skills in the organization.
- **Manual processes.** 56% of organizations say that things slip through the cracks because emails and spreadsheets are used to manage response processes.
- **Silos.** 62% of breached organizations were unaware that their organizations were vulnerable.

Automation accelerates IT and security response to incidents.

Companies with fully deployed automated security solutions are responding faster with collaboration across teams; 80% say they were able to respond to vulnerabilities in a shorter time frame. They are also saving the business an average of $2.5 million because they are able to see and respond to breaches faster. Conversely, banks not using automation lack visibility into what's happening in the business, which can result in costly breaches.

Figure 1: Most breaches were preventable but remained unaddressed



Automation also provides organizations with visibility into what's happening in the business, so that the organization can identify, prioritize, and mitigate issues before a breach occurs.

Why Automate?	
Identify	Centralized visibility of vulnerability data, business context, and risk
Prioritize	Increase productivity and reduce backlogs by attacking critical work first
Orchestrate	Automate workflow and ensure faster remediation

> From a simple capability to not only scale your teams but enable them to respond to vulnerabilities and incidents at near machine speed; that is an asset going forward.
>
> *Karl Klaessig, Director of Product Marketing, Security Operations, ServiceNow*

ADDITIONAL INFORMATION

For more information on contactless fraud, visit: https://leigh-annegalloway.com/

ServiceNow provides several resources focused on improving security operations.

- Security Operations Use Case Guide
- Costs and Consequences of Gaps in Vulnerability Response
- Accelerating Security Response

BIOGRAPHIES

Leigh-Anne Galloway

Head of Commercia Research, Cyber R&D Lab

Leigh-Anne Galloway is Head of Commercial Research at Cyber R&D Lab. She specializes in application and payment security. Leigh-Anne started her career in incident response, leading investigations into payment card data breaches, which is where she discovered her passion for payment technologies. She has presented and authored research on ATM security, application security, and payment technology vulnerabilities. Leigh-Anne has previously spoken at DevSecCon, BSides, Hacktivity, 8dot8, OWASP, Troopers, Black Hat USA, and Black Hat Europe.

Timur Yunusov

Head of Offensive Security Research, Cyber R&D Lab

Timur Yunusov is a Head of Offensive Security Research and a security expert in the area of banking security and application security. He regularly speaks at conferences and has previously spoken at CanSecWest, PacSec. DEF CON, Black Hat USA, and Black Hat Europe.

Karl Klaessig

Director of Product Marketing, Security Operations, ServiceNow

Karl is ServiceNow's Director of Product Marketing, Security Operations, and has over 15 years of experience in product positioning and marketing of enterprise security platforms, including SIEM, SOAR, and endpoint technologies, most recently from product marketing roles at RSA and McAfee, where he was responsible for the positioning of their security operations and automation platforms.