RFID Risk Analysis and Report

# Abraham Cain

# August 2, 2021

Contents

[Introduction 3](#_Toc78751696)

[Analysis 3](#_Toc78751697)

[Technology Use Case 3](#_Toc78751698)

[Privacy and Security Issues 5](#_Toc78751699)

[Recommendations 6](#_Toc78751700)

[Summary and Conclusions 9](#_Toc78751701)

[References 11](#_Toc78751702)

# Introduction

RFID is evidently coming into the spotlight as one of the newest and most attractive technologies for event management. Three of our teams at Padgett Beale are already on-board with implementing this technology for our events that we host. The benefits of RFID wristbands for events are great for our customers and could streamline our operations at events. Jessica Bowler of Printsome Insights (2016) notes that they can be used to quickly check guests in and track data on product consumption, times guests enter/leave, and where guests move around the events. ID&C (N.D.) notes that RFID wristbands can be used at resorts for contactless payment while doubling as a room key and even tripling as a ticket into the event or attraction. Token Team (2018) even says that RFID technology can even be tied into social media allowing attendees to post a picture of themselves at the event to social media with the tap of a wrist to a reader. There are plenty of reasons for them to want this technology on board. However, we should consider security and privacy risks that come along with this technology.

# Analysis

## Technology Use Case

This paper will analyze the following use case for the RFID technology. Individuals would use the RFID wristband to make purchases and to show identification for age verification. To have these capabilities, the wristbands must be able to store data or a token that can be used to fetch data. Sounds like an innocent use case, but we would need to gather at least the following personal/private information/data:

* Passholder name
  + cardholder name if different than passholder name
* Passholder birth date
* Passholder photo (photo of driver’s license or ID)
* credit card number
* billing address
* social media account information (optional)
* location data.

Jessica Bowler (2016) says in her article on Printsome Insights that RFID allows event organizers to track products being consumed, when/where attendees are coming and going. This can allow you to strategically place advertisements and refreshment stands. However, it may also create responsibilities for us to ensure the physical integrity of RFID readers across our facilities to ensure they are not compromised with skimmers.

Token Team (2018) recommends having using RFID wristbands to act as “digital wallets and go 100% cashless” (Section 5, Using RFID for cashless events) at your events. This gives attendees one less thing to lose: their wallets. However, this also quite literally makes people wear their wallets on their sleeves. If credit card numbers and PII are stored directly on the RFID tags, there is the possibility that criminals could hold an RFID reader to attendees’ wristbands while in a crowd and steal their information. We will attempt to mitigate this risk and others in the “Recommendations” section.

Intellitix (2012) displayed how the social media integration works with their RFID bands at the Bonnaroo festival. A user walks up to a photobooth and taps their wristband on the scanner. The booth then counts down and takes a picture to post to their social media account for them. The user links their social media account/s to the wristband before attending the event. This might bring up issues if people are caught in the background of the pictures and the photos are posted to social media without permission of the background persons.

## Privacy and Security Issues

If we are processing credit card payments using RFID wristbands, we have an obligation to maintain PCI DSS compliance. PCI DSS is a set of standards set forth by the Payment Card Industry and in our case, we would need to ensure Point to Point encryption of payment card information in transit (PCI SSC, 2017). If we fail to meet PCI compliance standards, we “may face fines up to $100,000 a month” says Ben Dwyer (2019) of CardFellow.

We also must consider that RFID can be read from about three feet away with the “Tastic RFID Thief” design by Fran (2013) and presented at DEFCON 2013 security conference. The reader is small enough to hide in a backpack and in a crowd of people, most would not notice a backpack being held at waist level three feet away. This creates a problem for the security of guests’ card data and PII as well as a problem for them and their bank with fraudulent transactions. Any attack on our patrons affects our reputation and guest trust of us as well.

Akin to skimming attacks, relay attacks are described by Ikuesanin Adeyemi and Norafida Ithnin (2012) in the paper “Users Authentication and Privacy control of RFID Card”. Adeyemi and Ithnin (2012) as a way of stealing information by placing a piece of malicious reader near the victim’s RFID token and another malicious transponder to bounce that signal next to the true reader acting almost like a long wireless cable between your RFID payment device and a point of sales terminal somewhere else. The main difference between these attacks is that the skimmers previously described take the data and store it, while the relay attacks simply bounce your data to a legitimate reader causing you to pay for their item or perform and action. It should be noted that this attack may be harder to pull off since it may require coordination with another person to use the malicious reader while you use the transponder.

Richmond Journal of Law and Technology notes that a bill was drafted by Senator Debra Bowen in 2004 that requires businesses to disclose to customers when they wish to collect data on them with RFID and obtain consent from the customer (Reuven R. Levary, et al, 2005). There are other laws like this in different US states. We should pay attention to those laws if we hold events at locations in other states/countries. We may need to have customers sign special permission forms or documents before gathering data on them using RFID wristbands.

We should keep in mind that if we operate in Europe, the GDPR regulation requires that we delete customer data when it is no longer needed for the purpose it was originally collected for, when the guest requests it be deleted, or when the data was collected without consent (Touch, 2017). We need to keep this in mind if we plan on storing data on customer spending habits and line queues around the park. It would be prudent to request consent for the specific reasons we are collecting their data and delete the data after the reasons are fulfilled.

Also, in the United States, the Sarbanes Oxley Act requires that companies “implement internal controls for adequately protecting customer financial information” (McAfee, N.D.). This affects us as we need to ensure that customer payment card information and financial information is kept safe to a reasonable degree. We also need to document proof that we are doing our part to secure their data and have an external registered auditor confirm this.

# Recommendations

Where there’s a problem, people will come together to solve it or work around it. To address the problems that arise from hackers using high-powered readers to sniff card data from their wristbands, we turn to tokenization. Georgina Park (2015) explains how tokenization works and can be used to decrease a company’s PCI scope meaning that it decreases our compliance risk. The following is a summary and application inspired by her definition in the article “How you can use tokenization to reduce PCI scope” on pcicompliance.org (Park, 2015).

By using tokenization, a customer is assigned a random string of numbers, letters, and symbols that is used in place of a credit card number at point of sales devices. When the customer wants to purchase an item, they use the token or an item that transmits their token (in our case an RFID wristband) and the token gets encrypted and sent to our databases where it is decrypted and used to retrieve cardholder information such as the card number and billing address from our secure database system.

This does a great job at defending against rogue readers and limiting our PCI DSS scope, however it won’t help us defend against relay attacks previously described.

A breakthrough in RFID security measures is the distance-bounding protocol described by Di Ma and Nitesh Saxena (2011) in their paper “A context-aware approach to defend against unauthorized reading and relay attacks in RFID systems”. They describe the protocol as

A cryptographic challenge-response authentication protocol that allows the verifier to measure an upper bound of its distance from the prover (Ma, Saxena, 2011).

In plain words, the protocol uses acute measurements of distance to the real RFID source to prove that a legitimate RFID token is being used and not a relay agent that would have a slight delay as the data would have to be bounced through two other devices.

Point to point encryption is typically needed to secure payment card data in the point of sales environment to be compliant with PCI DSS as previously mentioned. To address this, tokenization eliminates the liability of the cardholder data from our point of sales environment. However, we still need to think of the encryption and security needed at our payment processing facility or if we use a third party for this such as Square Payments (2014). It would be prudent to request proof of security from the provider as we are still responsible for the customer’s data. We can only transfer so much risk to the third party. Thus, it would be good to ensure that they have an encrypted channel in which you transmit the token data or PII and PCI from our website to their processing systems. If we choose to host our own PCI and PII databases, then we need to ensure secure encrypted communication channels between our point of sales terminals and data collection points and the databases and data correlation systems and networks. This may be achieved via the use of VPNs or other secure data transfer protocols such as an SSH tunnel, SFTP, and TLS protocols (Baykara, 2021). Even though PCI DSS states that we may use insecure protocols if layers of protection are implemented around them, there is no reason if we are building a new system that we can’t implement secure protocols at the very least to get the data from one network to the next.

In response to the data retention and deletion laws of GDPR brought up by Touch (2017), we should have data collection disclaimers when users use our website to register for their accounts and provide us with their personal and financial information. We need to disclose exactly what data we plan to collect, what we plan to do with it, and for how long. This gives the customers the power to decide whether they will allow us to collect and store their data and keep us out of hot water.

In response to SOX compliance concerns, we should ensure that we are documenting our security measures to be added into our financial report. We should also have these available in the case of an audit to show auditors that we are taking due care of customer information and ensure that we have a registered auditor reviewing our reports and practices. Having documentation isn’t enough though. It goes without saying that we need to actually implement these internal controls as well, not just document them as nice-to-haves.

# Summary and Conclusions

To summarize all that has been discussed, we have the following issues:

* Skimming (Rogue readers) and relay attacks
* Encryption requirements for PCI
* Data collection disclosure, permission, and deletion requirements for GDPR and state data privacy laws.

In response to these, we have the following guidelines/recommendations broken down by PPPT groups:

* People
  + Having a registered auditor evaluate our internal security controls and financial reporting
* Processes
  + Accurately document our internal security controls and accounting information
* Policies
  + Have data collection, use, and deletion disclosures/agreements provided to the customers when creating an account for the RFID program through our website
  + Delete customer information upon request
* Technologies
  + Use secure protocols for PII or PCI data transfers between our website or point of sales terminals to our databases and data processing center
  + Implement a distance-bounding protocol on RFID readers and RFID point of sales devices
  + Use tokens on RFID wristbands instead of storing customer data directly on devices.

We welcome collaboration from the legal/compliance team and accounting teams on cementing policies and processes that are related to their departments and fine-tuning them to meet the needs of our organization and cover exceptions and loopholes. We believe that this project can proceed with caution as long as we adhere to these guidelines and stay informed on any regulatory or legal changes in the use of RFID for our purposes.

# References

Adeyemi, I. R., & Ithnin, N. B. (2012). Users Authentication and Privacy control of RFID Card.

Baykara, S. (2021, March 26). What you should know about PCI compliant file transfer. PCI DSS Guide. Retrieved August 2, 2021, from <https://www.pcidssguide.com/what-you-should-know-about-pci-compliant-file-transfer/>

Bowler, J. (2016, December 30). RFID wristbands - the good, the bad and the ugly. Printsome Insights. <https://blog.printsome.com/rfid-wristbands-good-bad/>

Dwyer, B. (2019, November 7). PCI compliance for mobile devices. CardFellow. <https://www.cardfellow.com/blog/pci-compliance-for-mobile-devices/>

Emerging Technologies, PCI Security Standards Council. (2017, September). PCI Mobile Payment Acceptance Security Guidelines. PCI Security Standards. Retrieved August 1, 2021, from <https://www.pcisecuritystandards.org/documents/PCI_Mobile_Payment_Acceptance_Security_Guidelines_for_Developers_v2_0.pdf>

ID&C. (n.d.). 8 benefits of using RFID wristbands for resorts & attractions. Retrieved August 2, 2021, from <https://www.idcband.com/en-us/blog-us/8-benefits-of-using-rfid-wristbands-resorts-attractions/>

Intellitix. (2012, September 19). Intellitix - RFID Social Media Integrations at Bonnaroo [Video]. YouTube. <https://www.youtube.com/watch?v=tY_jQ1yyK7g>

Levary, R., Thompson, D., Kot, K., & Brothers, J. (2005). Radio frequency identification: Legal aspects. Richmond Journal of Law & Technology, 12(1), 8. <http://law.richmond.edu/jolt/v12i2/article6.pdf>

Ma, D., & Saxena, N. (2011). A context-aware approach to defend against unauthorized reading and relay attacks in RFID systems (DOI: 10.1002/sec.404). Wiley Online Library. <https://deepblue.lib.umich.edu/bitstream/handle/2027.42/109577/sec404.pdf>

Marsh. (2013, November 3). RFID reader snoops cards from 3 feet away. Hackaday. <https://hackaday.com/2013/11/03/rfid-reader-snoops-cards-from-3-feet-away/>

McAfee. (n.d.). Sarbanes-Oxley (SOX) Compliance Requirements. Retrieved August 2, 2021, from <https://www.mcafee.com/enterprise/en-us/about/cloud-compliance/sarbanes-oxley-encryption-compliance-requirements.html>

Park, G. (2015, April 4). How you can use tokenization to reduce PCI scope. PCI Compliance Guide. <https://www.pcicomplianceguide.org/how-you-can-use-tokenization-to-reduce-pci-scope/>

Square. (2014, December 8). Payment tokenization explained. Squareup. Retrieved August 2, 2021, from <https://squareup.com/us/en/townsquare/what-does-tokenization-actually-mean>

Token Team. (2018, January 4). The beginner's guide to RFID technology for events | Token blog. Token RFID. <https://www.gettoken.com/beginners-guide-rfid-technology-events/#cashless>

Touch. (2017, November 14). GDPR – What are your data deletion obligations? Touch Call Recording. <https://touchcallrecording.com/blog/45-gdpr-what-are-your-data-deletion-obligations>