

Sparkasse Bank – Tricky broken Card Bug on ATM

The story begins four weeks ago when I was going to withdraw some money from a bank in kassel (Germany). On that day, I randomly noticed in my wallet, that my bank card had a little fracture along the magnetic strip. So, I wanted to get a new card, but the nice employee at the bank informed me that I must use the card until it no longer works. I was a bit skeptical at first, but stowed my card away after my transaction.

One week later, I was invited over to a friend's and wanted to quickly grab some cash from the bank around the corner.

Day 1

I stuck the card in the reader and processed my debit withdrawal. When I was done, for security reasons, the card should have been ejected before I was actually given the money. The card comes out about a fourth of the way, then the card reader made a weird sound and sucked the card back in. Three times it partially ejected the card and sucked it back in, and finally kept the card as it could not successfully eject it.

Shortly after, the ATM showed "Temporarily not available." on the display and started blinking oddly. The funny thing was, while I was lightly tugging on the card, the card reader would release the card as much as I pulled. Had I a faster finger, I could have completed the transaction. It registered the transaction, no cash given, and the card was taken!!

I naturally went to the lady at the counter and explained the problem. She asked me what my name was and immediately ducked away into a room in the back where you can open the ATM's. In the meanwhile, I spoke with a middle-aged woman who had seen the whole thing and told her what had happened. She said, "It's not so bad. At least no one can get anything off your card." At the time, I was skeptical and asked her why, and she said that crazy junkies had stolen her card and made a withdrawal for over €1000 in cash with a forged signature. Today, she was obviously at the bank to see her money after it had been thirty days, a refund dictated by banks in the event of credit fraud/theft. She said she had gone to the police because of the incident and the officer entertained her with a statistic that this kind of thing happens to everyone nowadays at least once. At that moment, I could have gone into a full rage, and was doing so in my head, because of the actions of the workers right before my eyes. Shortly then, the lady came from the back room and told me that I hadn't put a card in the reader because there wasn't a card in the receiver box. I told her that wasn't possible because I put my card in and had made the transaction.

She was at her computer and checked her reader application, which said that there was not a card in the reader. Again, she shrunk into the back room with a coworker to take a look. What I'd especially like to note, is that she accessed my account without ever asking for any identification. I only told her my name. That was all to have access to my transaction history and my current financial standing. Ten minutes later, the employee came back and showed the back of the panel, telling me that I wasn't going to get my card back. She explained to me that I wouldn't get a card back today because it was stuck in the card return slot of the ATM.

However, another worker would come in tomorrow to get the card, because she couldn't do it without damaging it. A coworker had tried before with another customer, and it destroyed the card. The employee did offer me the withheld €30 with a signature. At that moment, I wondered what would have happened if I had not offered up my ID. I signed anyway.

Although, I knew that it would require to be authenticated. I used my last name for the signature, although I always have clear and legible handwriting. Everything went fine and I got my money, and would return the next day.

I was naturally quite frustrated with this branch, but regardless, I remained a model customer, hopeful, and held my composure.

Day 2

I woke up around 8:00am and heard my answering machine. I had missed three calls. I called the support number for Sparkasse, totally annoyed that at 11:00am, no one had checked on my issue. What's funny, is that the bank was only open until 1:00pm and then would be closed for the weekend. Because there was no direct number to the branch, I had to tell a woman on the support line which bank to contact. Instead of being directly connected with an employee at the branch, I was informed through an employee of the support line, that my card in the ATM would be destroyed. Had I asked to be put through to an employee at the branch, I would have been denied. Luckily, I knew that only someone there in the branch could have destroyed the card. The woman suddenly asked me if I wanted to apply for a new card. I hung up and made my way toward the bank.

As soon as I walked through the door, I randomly saw the same employee who told me four weeks ago that I could use my card with no issue. She called corporate and affirmed what the situation was, and the employee on the other line asked if they should charge me for the card. I was just about to lose it. The woman looked at me and told the person on the other line that they could not charge me for a new card.

Then the woman wanted to destroy my old card at the branch where my card had been stuck. I rejected that idea, specifically because I wanted my card back to show them exactly where the card could be damaged to reproduce the error. One should know that, normally, damaged or unauthorized cards are sent to the receiving box.

Day 4

I received a letter that said my card was destroyed and my account on that card would be set to zero. It was the weekend with no money. No data protection and all my accounts would be listed as 0,00€!

Kasseler Sparkasse - 34111 Kassel
Herrn
Benjamin [REDACTED]
[REDACTED]
34246 Vellmar

Geschäftsstelle Kirchditmold
Teichstr. 20
34130 Kassel

Martin Scheidler
Telefon: 0561 7124-5
Telefax: 0561 7124-7
kirchditmold@
kasseler-sparkasse.d

11.06.2010

Rücksendung Sparkassencard
Sehr geehrter Herr [REDACTED],
wie gewünscht senden wir Ihnen Ihre Sparkassencard wieder zu.
Das Chipguthaben beträgt 0,00€.

Bitte verwenden Sie die Sparkassencard nicht mehr an den Automaten, da durch den Riss
in der Karte die Automaten beschädigt werden könnten und dies verursacht Kosten.

Mit der Bitte um:

<input type="checkbox"/> Unterschrift	<input type="checkbox"/> Korrektur	<input type="checkbox"/> Stellungnahme
<input checked="" type="checkbox"/> Kenntnisnahme	<input checked="" type="checkbox"/> Bearbeitung	<input type="checkbox"/> Rückgabe
<input type="checkbox"/> Anruf/Rücksprache		

Zum Verbleib Mit Dank zurück Zur weiteren Verwendung

Mit freundlichen Grüßen
Kasseler Sparkasse
Martin Scheidler
Jeannette Schmelz-Katzwinkel

Day 6

I obtained a print out of my account history to see how it looked and to check it over.

http://hs03p.po.intern/zvp/ums/einst

Vertrag: [redacted] 359 / Privat giro / EUR / Umsätze: 02.06.2010 bis 17.06.2010 / Sortierung: Rückwärts
Vertragsinhaber: [redacted] Ber [redacted] (02 [redacted])
Saldo: [redacted] / Stand vom: 17.06.2010 17:47:15

Umsätze anzeigen

BuTag Valuta	Gg-Ktonr/ IBAN	Gg-BLZ/BIC	Auszugstext/Verw.-Zweck Name Gegenkonto	Betrag/Saldo WKZ	AZG	TS	US	PN
17.06.2010	0	5205 [redacted]	Barauszahlung	-50,00 EUR		03	00	
17.06.2010								
15.06.2010	901731 [redacted]	5205 [redacted]	EINBEHALTENES GELD GAA KIRC GAA GST 1 017	30,00 EUR		70	00	
15.06.2010								
15.06.2010	180478 [redacted]	600 [redacted]	BEITR. FR 6774 [redacted] 05.10 DEUTSCHE [redacted] WEST	-75,77 EUR		11	00	
15.06.2010								
14.06.2010	0	5205 [redacted]	Barauszahlung	-20,00 EUR		03	00	
14.06.2010								
10.06.2010	0	5205 [redacted]	Barauszahlung	-30,00 EUR		03	00	
10.06.2010								
10.06.2010	0	5205 [redacted]	10.06/17.17UHR KIRCHDITM GA NR00002368 BLZ52050353 0	-30,00 EUR		04	00	
10.06.2010								
08.06.2010	0	5205 [redacted]	08.06/17.20UHR VELLMAR-WE GA NR00 [redacted] BLZ52050353 0	-50,00 EUR		04	00	
08.06.2010								
08.06.2010	0	5205 [redacted]	08.06/14.40UHR VELLMAR-WE GA NR00 [redacted] BLZ52050353 0	-50,00 EUR		7	04	00
08.06.2010								
04.06.2010	0	5205 [redacted]	Kundenhinweis			7		
04.06.2010								

9 Einträge

Für eine Rückgabe wählen Sie bitte einen Rückgabegrund aus:

Umbuchung ausführen · Stornierung ausführen · Kontoauszugssicht · Zweitschrift drucken · Übersicht drucken · Rückg

After this happened to me, I could have previously answered this: <http://www.postpla.net/namen-gesetzes/sparkasse-kein-geld-automaten-bekommen-abgebucht.37971.html>@AnonymousUser: The ATM stood completely still after the error, and the next customer couldn't stick their card in or take the money out of the dispenser.

1. The card comes out before the money
2. The ATM, after the card entry and getting stuck, is completely worthless and waits on a technician, which, at the moment, can take up to 2 business days.
3. Also, after the card entry (and into the receiving box), the ATM is out of commission for a certain amount of time.

Good thinking, but why do you receive your money days later from the bank at the counter without authorization? I don't really know why that would happen to your account, but I got money out twenty minutes later without long analysis or ID. You're absolutely right! It would be practical to me to first yank the money out of the machine, and then dispense the same amount at the counter. Have you tried to pull the card out a little bit when the same happened to you? As everyone is aware of this issue, I couldn't double check to see if this works, as it could be a criminal offense.

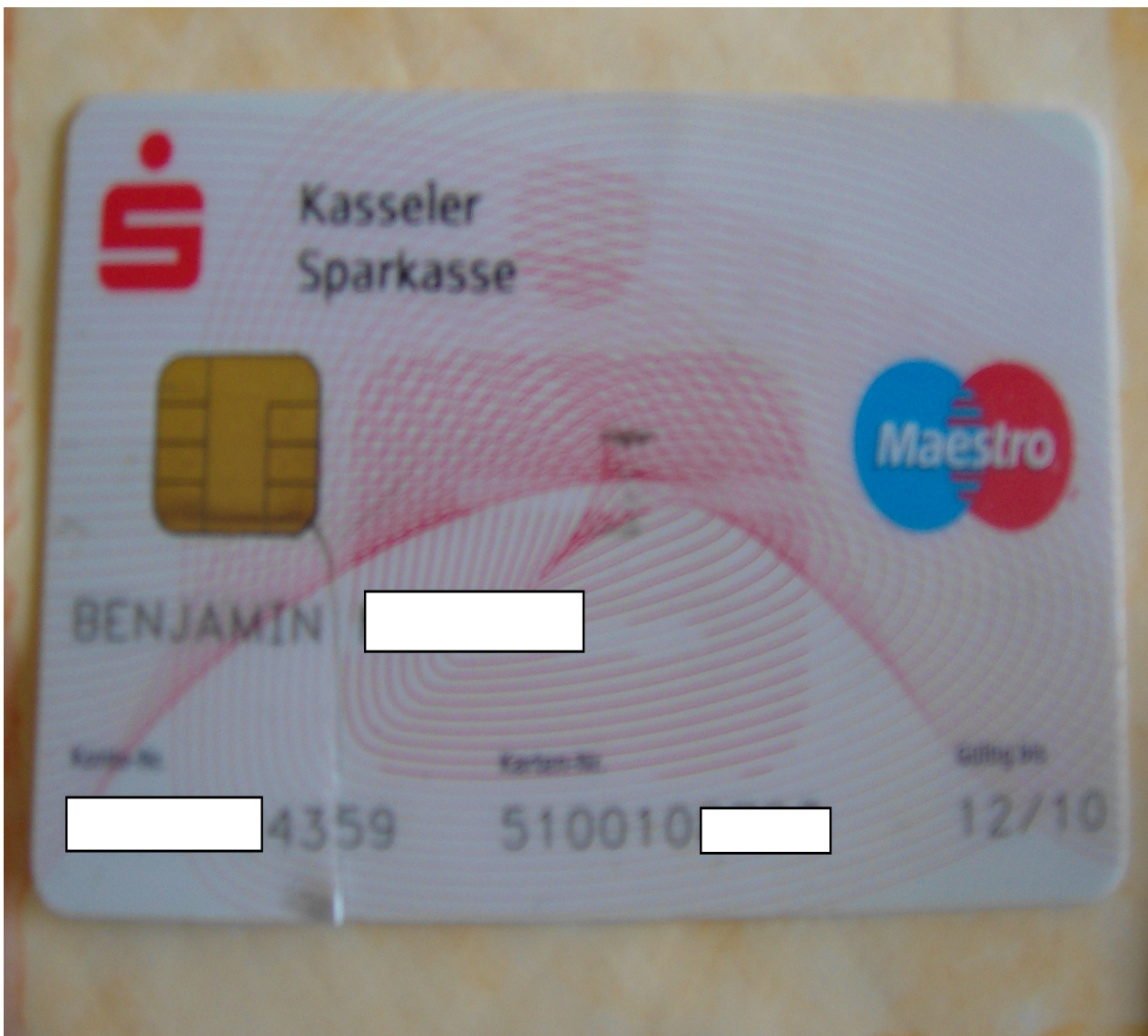
“Temporarily not available” – Is a broken card better than stolen?

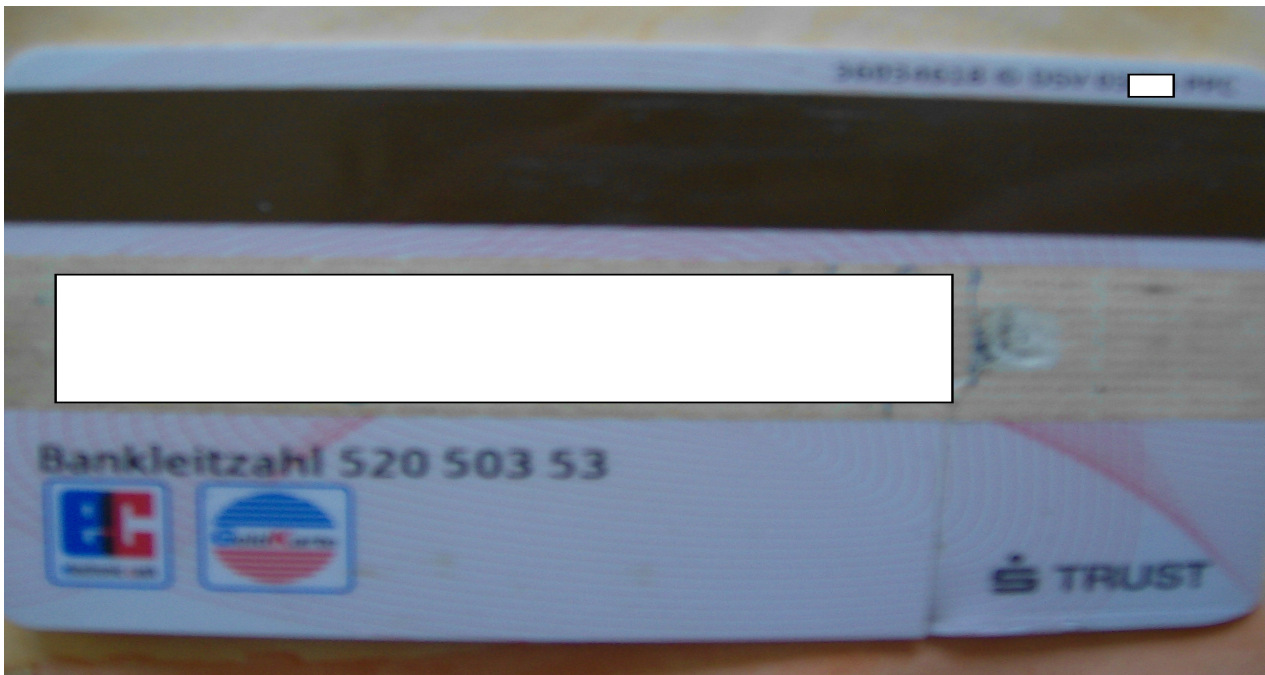
A misconfiguration bug is detected on the sparkassen atm & reception structure. A specific manipulated or broken card can lead to a bypass of the important output function – card before spending money. The bug allows an attacker to crash the automat at the end of the transaction on output to simulate a failed banking transaction. Bank staff are geared to a specific Theorie in such a case. A payout can take place so long as the card is not retained Card before spending money theory. The biggest problem is that the teller has no way of knowing if the customer received money from the ATM or not. A method must be found that can verify if the user did or did not receive money from the ATM and can be impervious to the majority of attacks that would disable this verification. Where there a check after the error but before the dispensing of money, the error wouldn't be an issue. But because there isn't one, the attacker could theoretically get the money and take the receipt to be cashed a second time.

“Temporarily not available”

1. One takes a card with the above details to an ATM. Put the card in the ATM and make a large withdrawal (€100-€280).
2. At the payout after the transaction, the card will get stuck.
3. Just wait patiently on the card and it would come out about a fourth of the way.
4. When the payout occurs, grab the money quickly and push the card back in again as it will want to take it.
5. The ATM will show “Temporarily not available” and is, until inspected, out of service.
6. Then bring the issue to the teller and get the exact money you tried to collect previously with the receipt in hand.
7. You can give whatever signature you’d like, as there will be no signature checks, and the camera will only capture your face. (Please note: You should probably eventually notify the employers to ask for identification first.)
8. ATM bank hack complete. Hail to the king, baby.

The trick of the thing is to not completely pull the card out, but instead leave it at the last sensor where it can remain hanging. If you’ve messed up that step, then just leave the card hanging and when the reader tries to read for a card again, just give it a little nudge and the card will be sucked in again. For the developer or manufacturer it looks like the transaction got canceled in the last instance of the payout! The Bank can not say you have taken the money or not till they have checked again the complete moneybox.





Additional Information:

I found this method randomly and had no malicious intentions. Manipulation of an ATM in conjunction with social engineering is a criminal activity! I don't suggest to anyone to commit a criminal act, even if it's just as a documentary or analysis of an every day event. It is forbidden to tamper or disable ATM's (Denial of Service), and could result in jail time for the perpetrator with evidence of malicious intent. **DO NOT TRY TO REPRODUCE THIS BUG BECAUSE YOU HAVE TO PAY ANY DAMAGE! DO NOT USE THIS INFORMATION FOR ANY CRIMINAL ACTIVITIES OR ACTIONS! [DOCUMENTATION]**

Contact: admin@vulnerability-lab.com

Support: support@vulnerability-lab.com

Research: research@vulnerability-lab.com

Submit Advisories: submit@vulnerability-lab.com

