Ergänzende Angaben zu einem „Betrugsvorfall beim Online-Banking“ als Anlage zur Strafanzeige der Polizei sowie Bearbeitungsgrundlage für das Kreditinstitut

Dienststelle	
Vorgangsnummer	
Aktenzeichen Staatsanwaltschaft (wenn bekannt)	
Kreditinstitut	
Aktenzeichen Kreditinstitut	

Straftatbestände:

- **§ 263 a StGB Computerbetrug (PKS 517500)**
  in Verbindung mit
- § 202 a StGB Ausspähen von Daten
- § 303 b StGB Computersabotage
- § 303 a StGB Datenveränderung
- § 261 StGB Geldwäsche

1. Angaben zum Betroffenen

Name	
Vorname	
Geburtsdatum/-ort	
Straße	
PLZ Wohnort	
Tel.-Nr.	
E-Mail-Adresse	
Zugangsnummer zum Online/ Telefon-Banking	
Betroffenes Konto	
Firmenkonto/Privatkonto	

gibt an, Geschädigter eines Betruges beim Online-Banking geworden zu sein

2. Online Banking

Folgende/s eigene Konto/-en sind/ist betroffen

IBAN	BIC	Name der Bank	Ort

Weitere Konten gesondert aufführen

Beim Vorfall benutzte ich folgendes TAN-Verfahren

☐ PIN/TAN (Transaktionsnummern (TAN) auf der Liste sind nicht durchnummeriert)
☐ iTAN (Indizierte Transaktionsnummern, TAN auf der Liste sind durchnummeriert)
☐ mTAN/SMS-TAN (mobile TAN, wird von Bank auf Handy des Kunden gesendet)
☐ eTAN (elektron. TAN, Kunde hat TAN-Generator, der elektron. eine TAN erzeugt)
☐ eTAN Plus (wie eTAN, zusätzlich Einbindung von Überweisungsdaten)
☐ HBCI/FinTS (Chipkarte und Lesegrät, USB am PC, wie EC Karte mit PIN)
☐ Photo TAN
☐ Push TAN über App
☐ Andere
☐ Ich benutze eine Banking-Software (z.B WiSo-Money/MeinGeld/Starmoney/Handy-App o.a.)
☐ Welche

Ich benutze keine Banking-Software sondern habe die Internetseite der Bank aufgerufen, indem ich

☐ Meinen Webbrowser gestartet und die Internetadresse in die Browserzeile eingegeben habe
☐ Das im Favoriten-Ordner oder Lesezeichen-Symbol gespeicherte Lesezeichen der Internetadresse der Bank angeklickt habe
☐ Auf einen Link einer E-Mail der Bank geklickt habe
☐ Sonstiges

Auffälligkeiten

☐ Mein eigentliches TAN-Verfahren wurde von unbekannt geändert
☐ Die zum Konto gehörende Mobilfunknummer wurde von unbekannt verändert
☐ Es kam zu vorherigen Transaktionen von Unterkonten auf mein Hauptkonto, die nicht von mir durchgeführt wurden

Ich bin

☐ Erstmalig
☐ Wiederholt

Opfer eines Betruges im Onlinebanking geworden.

3. Dateneingabe im vorliegenden Fall

Die Online-Banking-Sitzung habe ich am um Uhr begonnen

☐ Die Online-Banking-Sitzung wurde durch mich selbst durchgeführt
☐ Die Online-Banking-Sitzung wurde durch eine mir bekannte Person durchgeführt
☐ Dabei handelte es sich um
☐ Die Online-Banking-Sitzung wurde durch eine unbekannte Person durchgeführt
☐ Ich erhielt einen Anruf von einer Person und wurde telefonisch angewiesen
☐ Die Person hatte eine ☐männliche ☐weibliche Stimme
☐ Mir wurde im Telefonat suggeriert, dass ich Geld an einen ☐Bekannten, ☐einen Techniker oder ☐sonstigen Support überweisen sollte

☐ Die Transaktion wurde durch mich selbst durchgeführt
☐ Die Transaktion wurde durch eine unbekannte Person manipuliert
☐ Ich erhielt einen Hinweis auf eine Sicherheitsabfrage
☐ Die Daten auf der Überweisungsmaske waren bereits eingetragen
☐ Ich erhielt einen Hinweis auf eine Fehlüberweisung, welche zurück gebucht werden sollte
☐ Während der Sitzung öffnete sich ein weiteres Fenster mit sinngemäß folgendem Inhalt

☐ Während des Überweisungsvorgangs öffnete sich kein weiteres Fenster
☐ Ich habe folgende Daten in die Online-Maske der Internetseite eingetragen
☐ Kontonummer
☐ PIN
☐ TAN
☐ Sonstiges

4. Hardware/Software/Internet

Der Vorfall ereignete sich beim
☐ Telefon-Banking ☐ Browserbasierten Online-Banking
☐ Mobilen-Banking mit Smartphone/Tablet
☐ Sonstiges
☐ Benutzter Finanzsoftware
☐ Benutzter Hardware, welches von Kreditinstitut zur Verfügung gestellt wurde (z.B. HBCI)
☐ Sonstiges
Für das Online-Banking benutzte ich ein/-en ☐ PC ☐ Notebook ☐ Smartphone
☐ Sonstiges

Der **Zugang zum Internet** wurde hergestellt über ein/-en
☐ DSL-Anschluss ☐ Modem/ISDN ☐ Kabelanschluss ☐ Internetstick
☐ Mobilfunk ☐ Sonstiges

Ich befand mich zur Vorfallszeit
☐ Im heimischen Netzwerk ☐ In einem öffentlichen Netzwerk ☐ Auf der Arbeit
☐ Sonstiges

Mein **Internetprovider** ist
☐ Deutsche Telekom ☐ Vodafone ☐ O2 ☐ Kabeldeutschland
☐ Sonstige

Als **Betriebssystem** war zur Vorfallszeit installiert (Bezeichnung/Version eintragen, wenn bekannt)

Windows	
iOS	
Android	
Sonstige	

Aktualisiert wird das Betriebssystem
☐ Automatisch ☐ Manuell ☐ Unbekannt
Das für die Transaktion/-en benutzte Benutzerkonto hatte
☐ Administratorrechte ☐ einfache Benutzerrechte
☐ Gastrechte ☐ unbekannt
Eine **Antivirensoftware** ist
☐ Installiert ☐ Nicht installiert ☐ Kostenpflichtig ☐ Kostenfrei
☐ Welche
Eine Aktualisierung der Antivirensoftware erfolgt
☐ Automatisch ☐ Manuell ☐ Unbekannt
Letzte Aktualisierung

Letzte vollständige Systemprüfung durch den Virenscanner

Eine **Firewall** ist
☐ Installiert ☐ Aktiviert ☐ Deaktiviert
Die Aktualisierung der Firewall erfolgt
☐ Automatisch ☐ Durch Programm ☐ Durch Betriebssystem
☐ Manuell ☐ Unbekannt

5. Verhalten des PC

Nach Eingabe der Daten verhielt sich mein PC/Notebook/Smartphone folgendermaßen
☐ Überweisungsvorgang wurde unterbrochen
☐ Überweisungsvorgang wurde nicht unterbrochen
☐ PC „stürzte ab“ ☐ PC lief normal weiter
☐ Ich erhielt einen Hinweis auf eine Sicherheitsabfrage
☐ Ich erhielt einen Hinweis auf eine Rücküberweisung
☐ Eigene Sachverhaltsschilderung

Ich habe ☐ einen ☐ keinen Suchlauf durch das Antiviren-Programm unternommen

Das Antiviren-Programm hat
☐ Eine Schadsoftware ☐ Keine Schadsoftware festgestellt

Ich habe nach dem Vorfall das Betriebssystem
☐ Neu aufgesetzt ☐ Nicht verändert

Ein Virenreport/Trojanerreport
☐ Liegt bei ☐ Wird nachgereicht

6. Überweisungsdaten

Nach Einblick in die Umsatzliste des Kontos habe ich festgestellt, dass folgender Betrag/folgende Beträge missbräuchlich von meinem Konto abgebucht wurde/n (hier das „Zielkonto“ eintragen)

Datum der Transaktion	
Betrag	
IBAN Zielkonto	
BIC Zielkonto	
Name Empfänger Zielkonto	
Verwendungszweck	

Weitere Transaktionen gesondert erfassen

☐ Es kam zu Umbuchungen innerhalb meiner Konten, welche ich nicht authorisiert habe

☐ Es kam zu Verkäufen von Wertpapieren, welche ich nicht authorisiert habe

Der Betrag konnte durch die Bank
☐ Angehalten ☐ Zurück gebucht werden

7. Datensicherung

Ich bin damit einverstanden, dass durch die Polizei eine Kopie der Festplatte meines PC/Notebooks für weitere Ermittlungen erstellt wird

☐ Ja

☐ Nein

8. Sonstige Vermerke

9. Anlagen

☐ Kontobelege ☐ Überweisungsbeleg der Onlineüberweisung ☐ keine

☐ Andere

☐ Virenreport

10. Ermächtigung für die Datenanforderung beim Kreditinstitut des geschädigten Kontoinhabers

Ich/wir erklären uns damit einverstanden, dass mein/unser Kreditinstitut gegenüber den Ermittlungsbehörden die erforderlichen Auskünfte zu den angezeigten Transaktionen erteilt

Polizeiliche Vorgangsnummer	
Kontoinhaber	
Kreditinstitut	
IBAN	
BIC	

Datum (TT.MM.JJJJ)	Sachbearbeitende Dienststelle	Unterschrift Geschädigter/Kontoinhaber

Bearbeitungsnummer des Kreditinstitutes

Hinweis für den Sachbearbeiter des Kreditinstitutes

Es wird gebeten, Daten welche dem Kreditinstitut im Zusammenhang mit dem angezeigten Sachverhalt vorliegen, der ermittelnden Polizeidienststelle zeitnah, auf ein gesondertes polizeiliches Ersuchen hin, zur Verfügung zu stellen

WICHTIGER HINWEIS FÜR DEN ANZEIGENERSTATTER

Ursache für diese widerrechtliche Abbuchung ist ein heimlich eingeschleustes Schadprogramm auf Ihrem genutzten PC/Notebook oder Smartphone. Sorgen Sie zuerst für eine gründliche Überprüfung des Gerätes, bevor sie damit wieder Zugangsdaten im Internet nutzen!
Wichtige Informationen und eine Anleitung, wie Sie ihren genutzten PC/Notebook oder Smartphone säubern, erhalten Sie in dem Informationsblatt „Achtung! Schadprogramm!“, welches Sie auf den Internetseiten des „Ratgeber Internetkriminalität“

www.polizei-praevention.de

finden.
Auch wenn die Transaktion von ihrem Konto nicht erfolgt ist, liegt eine strafbare Handlung vor. Erstatten sie auch in diesem Fall unbedingt Anzeige. Beachten sie bitte auch in diesem Fall die Hinweise aus dem Merkblatt „Achtung! Schadprogramm!“

Herausgeber
Landeskriminalamt Niedersachsen, Zentralstelle Cybercrime, Am Waterlooplatz 11, 30169 Hannover

Stand: April 2016