LEARNING NUGGET
#5

Kartenbetrug schwer gemacht

Einführung und Einblicke in den Kartenmissbrauch
und seine erfolgreiche Bekämpfung

Die Debitkarte ist und bleibt sehr sicher. Die bisherigen Zahlungsmöglichkeiten (z. B. am Terminal im Laden) haben dank neuster Technologien eine äusserst niedrige Betrugsquote. Durch den Einsatz der Karten im E-Commerce-Bereich gewinnt das Thema Betrug ohne physische Karte jedoch laufend an Bedeutung. Die meisten Betrugsarten zielen dabei auf die grösste Schwachstelle ab: die Kartenbesitzer selbst.

Einführung

Kartenmissbrauch – nachfolgend auch «Fraud» genannt – ist der vollendete oder versuchte Betrug unter Verwendung einer Zahlkarte, wie z. B. einer Kredit- oder Debitkarte. Das Ziel der Betrüger kann darin bestehen, Waren, Dienstleistungen oder Bargeld zu erhalten. Der Betrug mit Zahlkarten ist so alt wie Zahlkarten selbst. Anfangs erfolgte er nur bei sogenannten Card-present-Transaktionen (auch Face-to-Face-Transaktionen genannt).

Seit die Möglichkeit besteht, Zahlkarten als Zahlungsmittel für Online-Einkäufe zu verwenden, und immer mehr Karteninhaber diese Funktion nutzen, hat sich auch der Schwerpunkt des Betrugs mit Zahlkarten auf Card-not-present- und Online-Transaktionen verlagert.

- **«card present»** – rund 6% aller betrügerischen Transaktionen: Die physischeKarte wird verwendet (per Magnetstreifen oder Chip), um eine Zahlung vor Ort zu tätigen, z. B. an einem Bancomaten, in einem Ladengeschäft, einem Restaurant oder einem Supermarkt.

- **«card not present» (CNP)** – rund 94% aller betrügerischen Transaktionen: Nur die Daten der Karte werden verwendet, die physische Karte selbst wird vom Käufer jedoch nicht vorgelegt. Beispiele: Manuelle Eingabe der Daten im Internet, am Telefon oder an einem Terminal in einem Geschäft.

Dank moderner, selbstlernender Präventionssysteme und ausgefeilter Regelwerke sowie der langjährigen Erfahrung von Fraud-Analysten und Fachexperten können diese Betrugsarten stark eingedämmt werden.

Zunehmende Nutzung von E-Commerce mit Auswirkungen auf Betrugsmuster

Im Jahr 2018 wurden 10% aller Transaktionen weltweit online getätigt, bis 2022 werden die Ausgaben im E-Commerce 17% aller Umsätze weltweit ausmachen (Quelle: Ravelin Insights).

Im Jahr 2020 haben Online-Transaktionen nochmals deutlich zugenommen, unter anderem infolge der Lockdowns während der Corona-Pandemie. Dabei war ein verändertes Betrugsmuster zu beobachten, wie interne Analysen der Acquiring-Dienstleister Worldline und von SIX bestätigen. Während die Anzahl der betrügerischen Transaktionen insgesamt zunimmt, hat sich der durchschnittliche Betrugsbetrag pro Transaktion im Vergleich zu den Vorjahren reduziert. Die Betrüger passen ihre Vorgehensweise geschickt an unverdächtige Zahlungsmuster von Karteninhabern an, wodurch der Betrug schwerer zu erkennen ist. Exemplarisch dafür ist die Betrugsmasche des sogenannten «Hungry Fraudster». Dabei handelt es sich um Bestellungen bei Essens-Lieferdiensten über zahlreiche, aber geringe Beträge, die gezielt über mehrere Tage verteilt werden. Die Kartenbelastungen sollen nach Möglichkeit nicht oder erst mit Verspätung auffallen.

Kartenmissbrauch ist ein ständiger Wettlauf zwischen Betrügern auf der einen und Zahlungsdienstleistern auf der anderen Seite: Betrüger suchen beständig nach neuen Betrugsmöglichkeiten, Issuer und Acquirer sind ununterbrochen gefordert, neue Schutzmassnahmen zu ergreifen und Betrugsversuche zu vereiteln.

Betrüger und ihre Betrugsmaschen

Unter dem Schlagwort Darknet versteht man ein anonymes Netzwerk, das einen verborgenen Teil des öffentlichen Internets darstellt. Kriminelle – sogenannte Fraudster – können hier anonym miteinander interagieren. Sie versuchen, sich so dem Zugriff einer Aufspürung durch die Polizei zu entziehen. In Darknets kaufen und verkaufen Betrüger Kartendaten und tauschen Informationen darüber aus, wie sie einen Betrug begehen und welche Tools zu verwenden sind. Es handelt sich um eine wachsende Form organisierter Kriminalität mit eigenem Geschäftsmodell und effizienter Arbeitsteilung.

Welche Faktoren begünstigen diese Form der Kriminalität?

Gelegenheit und niedrige Eintrittsbarrieren: Anonym einen geeigneten Browser herunterzuladen, auf einschlägige Seiten im Darknet zuzugreifen und einen Kauf von Kartendaten in Kryptowährung zu tätigen, ist relativ unkompliziert.

Veränderte Strukturen: Das Bild des raffinierten Hackers, der mithilfe besonderer Fähigkeiten die Kontrolle über einen Server übernimmt, ist teilweise überholt. Bei Kartenmissbrauch handelt es sich heute um Straftaten, die keine besonderen Kenntnisse oder Fertigkeiten erfordern, sondern lediglich die Eingabe von Daten auf Webseiten oder in Apps. Auffällig ist, dass sich die gesamte Branche zunehmend professionalisiert und regelrechte Dienstleistungspakete anbietet, die neben der programmierten Schadsoftware alles für die Durchführung eines Hackerangriffes bietet.

Fehlende Stigmatisierung: Eine ganze Generation ist mit dem kostenlosen Herunterladen von Filmen, Musik, Spielen und Software aufgewachsen. Die Abgrenzung zur illegalen Beschaffung ist nicht immer leicht erkennbar und die Hemmschwelle zu einem Online-Betrug könnte dadurch gesunken sein.

Sorgloser Umgang mit persönlichen Daten, insbesondere in sozialen Netzwerken: Kartenbetrüger tummeln sich mit Vorliebe in sozialen Netzwerken, um an persönliche Daten von Karteninhabern zu gelangen. Beispiele dafür sind nachfolgend unter «Social Engineering» aufgelistet. Deshalb ist es entscheidend, dass Karteninhaber grundlegende Sicherheitsmassnahmen ergreifen und im Umgang mit persönlichen Daten Vorsicht walten lassen.

Mangelnde Kooperation: Kartenbetrug wird als Offizialdelikt eingestuft, das Strafverfolgungsbehörden von Amts wegen verfolgen müssen. Mit einer Anzeige bei der Polizei werden deren Ermittlungen und die Suche nach potenziellen Betrügern unterstützt. Jedoch werden der Polizei längst nicht alle Delikte gemeldet. Bei einer Online-Straftat sind Beweise zudem schwieriger zu erbringen als bei einem Diebstahl in einem Geschäft. Auch die Identifizierung von Tätern erweist sich häufig als schwierig. Das gilt insbesondere dann, wenn sich die Betrüger oder geschädigte Person in einem anderen Land als der Online-Händler befindet. Umso wichtiger ist daher eine Kooperation aller beteiligten Parteien (Karteninhaber, Issuer, Acquirer, Card Schemes, Behörden).

Übersicht über gängige Vorgehensweisen der Täter (Modus Operandi)

Die zunehmende Verlagerung von Kartenmissbrauch auf den Bereich E-Commerce zeigt sich anhand der am häufigsten vorkommenden Betrugsversuche:

Social Engineering:

- **Phishing:** Methode, um auf betrügerische Weise an private Informationen zu gelangen. In der Regel sendet der Betrüger eine E-Mail-Nachricht, die scheinbar von einem seriösen Unternehmen stammt, z. B. einer Bank oder einem Kartenunternehmen. Darin fordert der Absender die Überprüfung von Informationen und warnt vor schlimmen Folgen, falls die Angaben nicht gemacht werden. Die Nachricht kann auch einen Link zu einer betrügerischen Website enthalten, die unverdächtig erscheint. Weitere Beispiele sind hier Paketankündigungen («Um Ihnen das Paket zustellen zu können…») oder Fake Gewinnspiele («Sie haben gewonnen…»).
- **Spear-Phishing:** Die Vorgehensweise unterscheidet sich insofern von anderen Phishing-Angriffen, als stark individualisierte E-Mail-Nachrichten an ausgewählte Endbenutzer gesendet werden. Um überzeugender zu wirken, stellen die Betrüger zuvor zusätzliche Nachforschungen über potenzielle Opfer an.
- **Vishing (Voice-Phishing):** Bei dieser Vorgehensweise wird in krimineller Absicht versucht, durch Social Engineering per Telefon an private, persönliche und finanzielle Informationen zu gelangen.
- **Smishing (SMS-Phishing):** Bei dieser Vorgehensweise wird per SMS-Nachrichten versucht, die Opfer zur Preisgabe von persönlichen oder vertraulichen Daten zu bewegen.

Data compromise (Falsche Angebote und Schadsoftware):

- **Fake Apps:** Apps für Mobilgeräte, die Benutzer zum Herunterladen und Installieren verleiten. Die Apps sind als echte und attraktive Apps aufgemacht, die interessante Dienste anbieten. Sobald sie allerdings auf einem Mobilgerät installiert sind, können sie eine Vielzahl von Schäden verursachen.
- **Fake Websites:** Auf gefälschten Websites sollen Kunden dazu verleitet werden, vertrauliche Informationen preiszugeben, Malware herunterzuladen oder Produkte zu kaufen, die nie geliefert werden.
- **Malware:** Schadsoftware, die darauf abzielt, ein Computersystem zu stören, zu beschädigen oder sich Zugang dazu zu verschaffen.

Weitere bekannte Vorgehensweisen:

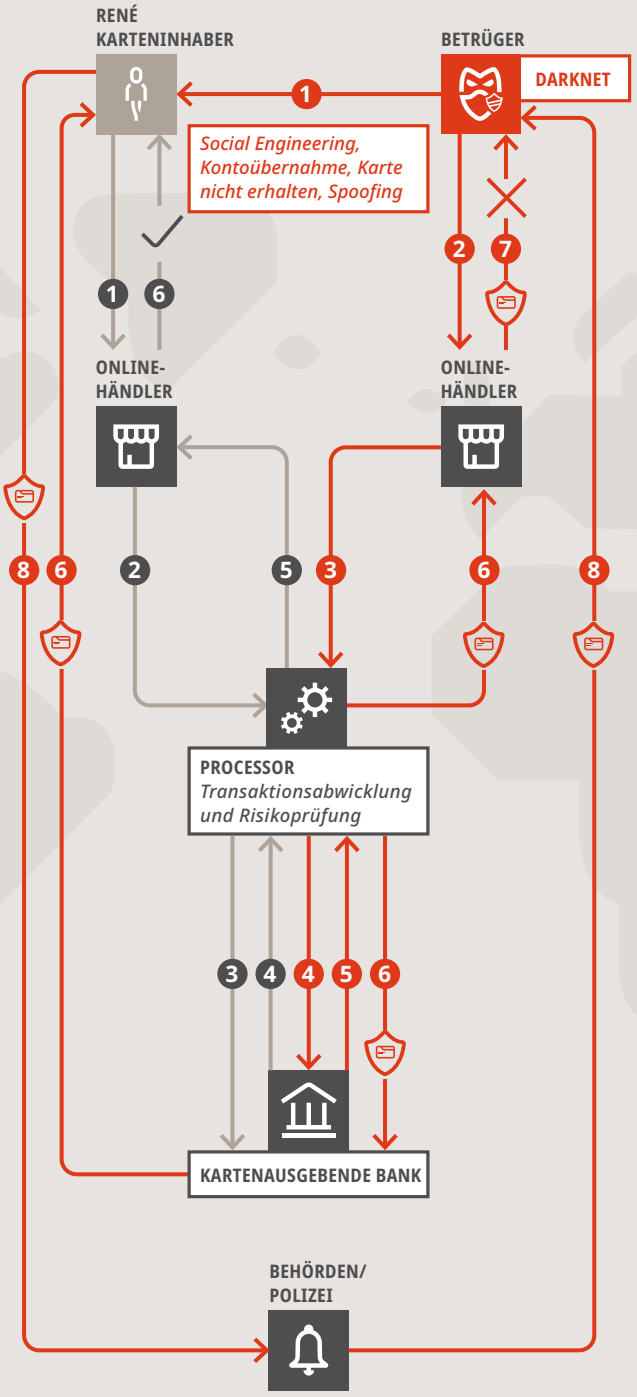
- **E-Skimming:** In diesem Fall wird die Kaufabwicklung von Online-Shops mit Malware infiziert, um Zahlungs- und persönliche Daten von Kunden während des Bezahlvorgangs auszuspähen.
- **Angriff auf die Kartennummer:** Betrüger verwenden die ersten sechs bis acht Ziffern einer Zahlkarte und errechnen mittels einer Software die restlichen möglichen Zahlen.
- **Account-Takeover-Fraud oder Account Hijacking (Kontoübernahme):** Eine Form von Identitätsdiebstahl, bei der sich die Täter erfolgreich Zugang zu den Anmeldedaten eines Benutzerkontos verschaffen.
- **Rückerstattungsbetrug (auch bekannt als Chargeback Fraud) und Friendly Fraud:** In diesem Fall behauptet ein Karteninhaber, dass weder er selber noch jemand aus seinem Haushalt, Waren oder Dienstleistungen online gekauft bzw. erhalten hat, um eine Rückerstattung zu erhalten.
- **Smurfing:** In diesem Fall tätigen Betrüger über einen längeren Zeitraum mehrere kleine Transaktionen, um möglichst lange unentdeckt zu bleiben (auch eine häufige Vorgehensweise bei Geldwäscherei).
- **Data Breach (Datendiebstahl):** Daten werden von einem System entwendet, ohne dass der Eigentümer des Systems davon weiss und sein Einverständnis gegeben hat.
- **Spoofing:** Bei dieser Vorgehensweise wird ein Kommunikationsvorgang (z. B. eine E-Mail-Nachricht, ein Telefonanruf) von einer unbekannten Quelle technisch als von einer bekannten, vertrauenswürdigen Quelle (Absender, Rufnummer) stammend getarnt.

Wie und wo kommt es zu Kartenbetrug?

Sind Betrüger im Besitz von Kartendaten und möglicherweise Passwörtern oder PINs, könnte ein Betrugsversuch wie folgt ablaufen:

Legitime Kartentransaktion

1. René erwirbt online ein neues Mobiltelefon.
2. Der Online-Händler leitet die Transaktionsanfrage über seinen Processor zur Prüfung weiter. Die Autorisierungsanfrage durchläuft automatisch die hinterlegten Regelwerke.
3. Die Autorisationsanfrage wird an die kartenausgebende Bank weitergeleitet.
4. Nach erfolgreicher Verifikation durch die Bank wird dem Processor die Freigabe zurückgemeldet.
5. Der Processor konsolidiert die Rückmeldungen der Bank und der Risikosysteme und meldet dem Händler die Transaktionsfreigabe zurück.
6. Der Kauf kann erfolgreich abgewickelt werden.



Missbräuchliche Kartentransaktion

1. Dem Betrüger gelingt es, an die persönlichen Karten- und Zugangsdaten von René zu gelangen.
2. Der Betrüger bestellt missbräuchlich Waren im Internet.
3. Der Online-Händler leitet die Transaktionsanfrage über seinen Processor zur Prüfung weiter. Die Autorisierungsanfrage durchläuft automatisch die hinterlegten Regelwerke.
4. Die Autorisationsanfrage wird an die kartenausgebende Bank weitergeleitet.
5. Nach erfolgreicher Verifikation durch die Bank wird dem Processor die Freigabe zurückgemeldet.
6. Der Processor konsolidiert die Rückmeldungen der Bank und der Risikosysteme. Die Transaktion wird präventiv abgelehnt, weil die Prüfung ein ungewöhnliches Kaufverhalten für dieses Kartenprofil ergibt.
   Je nach Regeldefinition kann die Karte zusätzlich vorübergehend gesperrt werden. Im Monitoring-Tool wird ein Betrugsalarm ausgelöst, der von Analysten überprüft wird. Die kartenausgebende Bank wird über die Transaktion informiert und kontaktiert den Karteninhaber zur weiteren Fallanalyse und zur Abstimmung des weiteren Vorgehens.
7. Der Online-Händler lehnt den Kauf ab. Der Betrugsversuch wurde erfolgreich verhindert.
8. Mit einer Anzeige unterstützen Karteninhaber die Polizei bei ihren Ermittlungen und bei der Suche nach potenziellen Tätern und Betrügern.

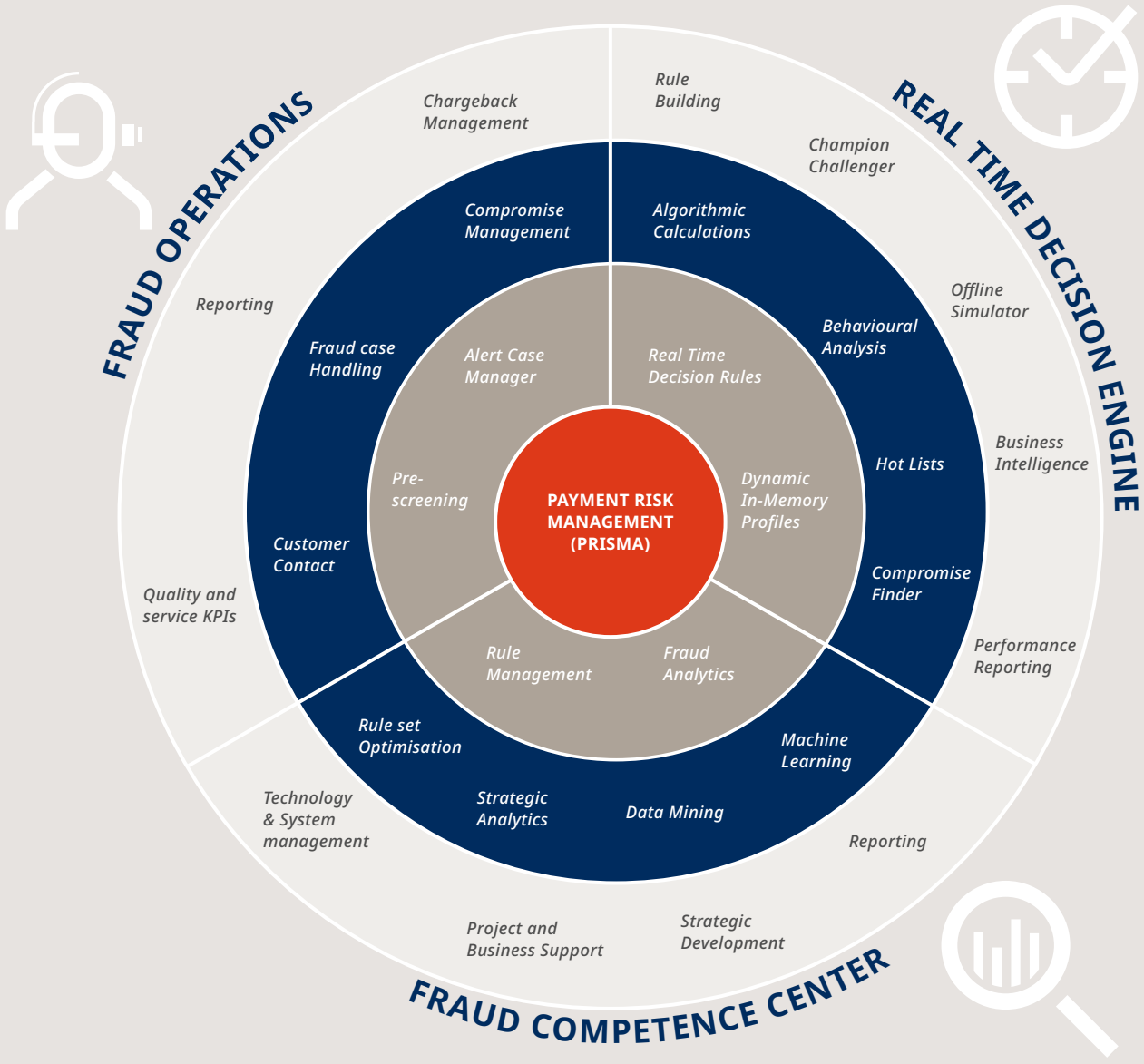
Wie lässt sich Betrug erfolgreich bekämpfen?

Die gesamte Payment Industrie setzt bei der Betrugsbekämpfung auf Echtzeit-Systeme, die mithilfe von selbstlernenden Technologien und aktivem Regelmanagement dynamisch und schnell auf neue Betrugsmuster reagieren.

Fraud-Experten (Data Scientists, Regeladministratoren und Fraud-Analysten) können neue und veränderte Betrugstendenzen zeitnah erkennen und proaktiv bekämpfen. Dabei werden die verwendeten Regeln zur Betrugserkennung laufend optimiert, damit höchste Sicherheitsanforderungen gewährleistet sind.

Zusammen mit Fraud-Operations-Teams, die als Schnittstelle zwischen dem Fraud Competence Center, dem Kartenausgeber (Issuer) und den Card Schemes fungieren, wird sichergestellt, dass Karteninhaber bei verdächtigen Transaktionen proaktiv kontaktiert bzw. bei bestätigtem Kartenmissbrauch optimal unterstützt werden.

Payment Risk Management (PRISMA) von SIX



Einige Massnahmen zur erfolgreichen Erkennung und Bekämpfung von Kartenbetrug

Karteninhaber	Processor/Issuer	
	Eingesetzte Technik:	Menschliche Intelligenz: Erfahrung von Fraud-Experten
– Aktivierung von 3DS (siehe Learning Nugget 3D Secure) – Geografische Einstellungen für die Einsatzregion der Karte anpassen (Geoblocking) – Setzen von Betragsgrenzen für die Karte wie Tages- oder Monatslimiten – Vertraulicher Umgang mit Kartennummer und Passwörtern/PINs – Gesundes Misstrauen beim Öffnen und Beantworten von E-Mail- und SMS-Nachrichten (Phising, Smishing): Absender genau prüfen und bei Links Mouse-Over benutzen bevor man klickt – Einkäufe nur auf vertrauenswürdigen Seiten: auf das «s» in der URL achten: «https://....» – Verwendung von starken Passwörtern und von unterschiedlichen Passwörtern für verschiedene Websites – Software und Geräte laufend aktualisieren (d. h., immer die jeweils aktuelle Version von Betriebssystem, Anwendungen, Virenscannern usw. verwenden) – Vorsicht bei Anrufen (bei Unsicherheit selber direkt auf offizielle Rufnummer zurückrufen)	**Verwendung hochmoderner Software:** – Echtzeit-Monitoring aller Zahlungsautorisierungen – Nahezu-Echtzeit-Monitoring aller Autorisierungs- und Clearing-Vorgänge – Profiling des Transaktionsverlaufs – Automatisierte Kartensperrung – Automatisierte Ablehnung von verdächtigen und missbräuchlichen Transaktionen – Regelmässige Aktualisierung des Regelwerkes im Fraud Monitoring Tool (bei Bedarf täglich) aufgrund von neuen Betrugsmustern und Analysen (z. B. nicht erkannte Betrugsfälle) oder Hinweisen von Fraud Investigators (auch neue Anforderungen der Card Schemes können Anpassungen erforderlich machen) – White-/Grey-/Blacklist – Intensiver Informationsaustausch zwischen den Beteiligten bei einem Vorfall (Verdachtsfall, Kartenmissbrauch, neue Betrugsmasche) – Nutzung von Tokenisierung zur Verschlüsselung von Karteninformationen (mehr dazu siehe Learning Nugget «Tokenisierung für Debitkarten») – Prüfung eingehender Transaktionen mithilfe von künstlicher Intelligenz unter Berücksichtigung von Regeln, bekannten missbräuchlichen Transaktionen, Verhaltens- und Betrugsmustern mit Alarm bei Abweichungen	**Fraud-Analysten:** – Untersuchung aller im System ausgelösten Alarme – Erkennung von neuen Betrugsmustern – Intensiver Erfahrungsaustausch unter Fraud-Experten, um immer auf dem neuesten Stand zu sein – Analyse von Gemeinsamkeiten zwischen ähnlichen Fraud-Fällen (z. B. CPP – Common Point of Purchase: wo wurde die Karte kompromittiert), um bisher noch nicht gemeldete Fälle von Kartenmissbrauch zu entdecken – Hinweise für Regelanpassungen – Intensiver Austausch mit kartenausgebenden Banken (Issuers) – Unterstützung der Behörden im Zusammenhang mit Kartenmissbrauch **Regeladministratoren und Data Scientists:** – Analyse von gemeldeten missbräuchlichen Transaktionen – Auswertung der Hinweise durch Fraud-Analysten – Simulieren und Testen von neuen Regeln und Regelanpassungen – Komplexe Analysen unter Berücksichtigung aller verfügbaren Daten – Erstellung von Statistiken/Berichten – Erstellen von Modellen im Zusammenhang mit künstlicher Intelligenz

FAZIT: DEBITKARTEN SIND UND BLEIBEN SICHER

Die Debitkarte ist und bleibt sehr sicher. Die bisherigen Zahlungsmöglichkeiten (z. B. am Terminal im Laden) haben dank neuster Technologien eine äusserst niedrige Betrugsquote. Durch den Einsatz der Karten im E-Commerce-Bereich gewinnt das Thema Betrug ohne physische Karte jedoch an Bedeutung.

Zahlungsdienstleister setzten bei der Betrugsbekämpfung auf Echtzeit-Systeme, die mithilfe von selbstlernenden Technologien und aktivem Regelmanagement dynamisch und schnell auf neue Betrugsmuster reagieren.

Kern der erfolgreichen Bekämpfung von Kartenmissbrauch ist ein enges Zusammenspiel zwischen Technik und menschlichem Know-how. Dank solider Netzwerke unter Zahlungsdienstleistern und koordinierter Aktionen mit Behörden wie Europol und Interpol gelingt es regelmässig, international agierende Banden zu stoppen, Marktplätze im Darknet auszuheben und Täter zu verhafteten.

Den besten Schutz vor Betrügereien bietet Prävention. SIX arbeitet seit Jahren sehr eng mit der Polizei zusammen. Gemeinsam mit Kartenausgebern betreiben wir die Präventionsplattform card-security.ch, die Karteninhaber und die Öffentlichkeit über verschiedene Kanäle über das Thema Kartensicherheit informiert und aufzeigt, wie man sich vor Missbrauch schützen kann.

WEITERE INFORMATIONEN HIER

SIX BBS AG
Hardturmstrasse 201
Postfach
8021 Zürich
T +41 58 399 4012