Neue Heraus- und Anforderungen beim Aufbau eines funktionierenden Compliance-Systems im Bereich der Exportkontrolle

- Exemplarisch verdeutlicht anhand des (US-)amerikanisch-deutschen Rechts- und Warenverkehrs und unter besonderer Berücksichtigung strafrechtlicher Tendenzen -

Rechtsanwalt Dr. Ulrich Wastl
Rechtsanwalt Dr. Philippe Litzka

Vortrag anlässlich der 5. Sitzung des Arbeitskreises Zoll und Außenwirtschaft der IHK

Black lists:

Debarred Parties
Office of Defense Trade Control (DTC)
http://www.pmddtc.state.gov/

Denied Persons List
Bureau of Export Administration
http://www.bis.doc.gov/DPL/Default.shtm

Entity List
Bureau of Export Administration
http://www.bis.doc.gov/Entities/Default.htm

Specially Designated Nationals List
Office of Foreign Assets Control (OFAC)
http://www.ustreas.gov/ofac/

Fallgestaltung 1:

Ausweitung der Zuständigkeit von US-Behörden auf „ausländische“ Sachverhalte:

a) „U.S. Person“ im Ausfuhrecht (Part. 772 EAR)
b) „U.S. Person“ im FCPA (15 U.S.C. §§ 78 dd)
c) „U.S. Person“ im Bereich der Geldwäsche

Fallgestaltung 2:

Informationsverschaffung

a) Händlerbeziehungen zwischen US-Firmen und Dritten

b) Programme der US-Behörden

1: Personnel Security

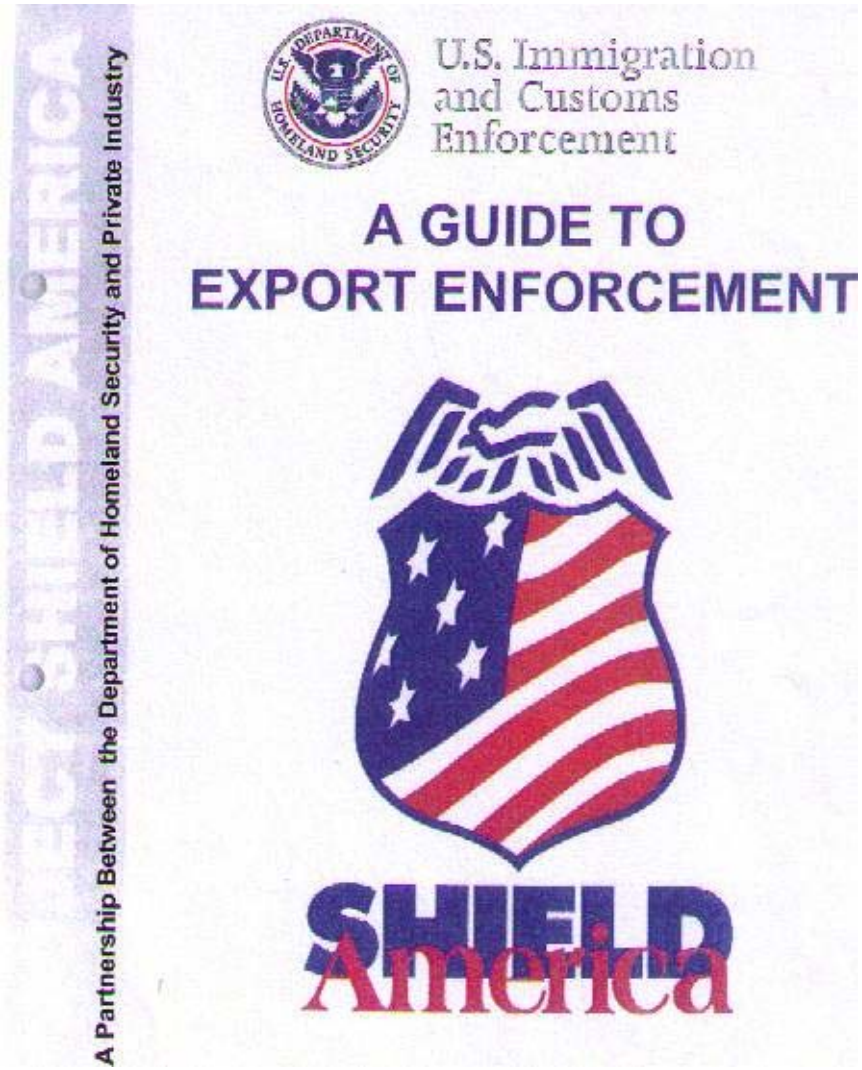
1.1	○ Yes ○ No	Before your company hires a person, does your company require the person to complete a written job application?
1.2	○ Yes ○ No ○ NA	Do you verify work history and references stated on applications submitted by job applicants?
1.3	○ Yes ○ No	Are you permitted by your government to conduct background checks on prospective employees?
1.4	(Select all that apply) ○ Not Applicable - Do Not Conduct Background Checks ○ Criminal Background Check ○ Financial Background Check/Credit Report ○ Drug and Alcohol Testing ○ Driver History ○ Unexplained Gaps or Periods of Unemployment ○ All of the Above ○ None of the Above	Do you screen job applicants using the following background checks?
1.5	○ Yes ○ No	Do you have a written code of conduct or policy that addresses security violations by employees?
1.6	○ Yes ○ No	Does your government allow your company to do background checks on existing employees?

4: Procedural Security

4.1	○ Yes ○ No	Do you notify your foreign customers and supply revised commercial documentation in the event of changes to the actual shipped goods or changes in the actual quantity of goods being shipped?
4.2	○ Yes ○ No	Do you provide commercial documentation to the foreign freight consolidator or carrier prior to actual exportation from the port of lading?
4.3	○ Yes ○ No	Do you verify the quantity of product being shipped against purchase orders?
4.4	○ Yes ○ No	Do you positively identify drivers delivering or receiving cargo before cargo is received or released?
4.5	○ Yes ○ No	Do you have procedures to ensure products are properly marked, weighed, counted, and documented?
4.6	○ Yes ○ No	Do you have procedures for tracking the timely movement of goods?
4.7	○ Yes ○ No	Do you have procedures for notifying Customs and/or local law enforcement agencies in cases where unusual incidents or illegal activities are detected or suspected?
4.8	○ Yes ○ No	Do you review security procedures on a periodic basis to prevent unauthorized access to facilities, equipment, and cargo?
4.9	○ Yes ○ No	Do you have internal controls for the selection of vendors/subcontractors?
4.10	○ Yes ○ No	Do you have written security standards or requirements for your vendors/subcontractors?
4.11	○ Yes ○ No	Do you use financial assessments to evaluate your vendors/subcontractors?
4.12	○ Yes ○ No	Do you discuss security issues with your vendors/subcontractors?

5: Information Technology Security

5.1	○ Yes ○ No	Do your employees use a computer system?
5.2	(Select all that apply) ○ Not Applicable - Do Not Have Computer Systems ○ Individual Accounts and Passwords are Created for Each Employee ○ Passwords are Changed Periodically ○ Computer Security Policies and Procedures Have Been Written ○ Employees Have Been Trained on Computer Security Rules ○ System Access is Monitored ○ Employees Who Violate System Rules Can be Punished ○ Firewalls and/or Anti-virus Software Used ○ Other Computer Security ○ All of the Above ○ None of the Above	Are your computer systems protected with the following security measures?



Westpfahl&Spilker

Contact Us
- Your Local FBI Office
- Overseas Offices
- Submit a Crime Tip
- Report Internet Crime
- More Contacts

Learn About Us
- Quick Facts
- What We Investigate
- Natl. Security Branch
- Information Technology
- Fingerprints & Training
- Laboratory Services
- Reports & Publications
- History
- More About Us

Get Our News
- Press Room
- E-mail Updates
- News Feeds

Be Crime Smart
- Wanted by the FBI
- More Protections

Use Our Resources
- For Law Enforcement
- For Communities
- For Researchers
- More Services

Visit Our Kids' Page

Apply for a Job

Counterintelligence Domain Program

The challenge: to protect United States sensitive information, technologies, and thereby competitiveness in an age of globalization.

Our solution: to foster communication and build awareness through partnerships with key public and private entities by educating and enabling our partners to identify what is at counterintelligence risk and how to protect it. We call it "knowing your domain"—identifying the research, information, and technologies that are targeted by our adversaries and establishing an ongoing dialogue and information exchange with partners to change behaviors and reduce opportunities that benefit the opposition's efforts.

The United States is the world's leader in innovation. Consider the breakthrough research and development that's taking place on the nation's campuses and in research facilities—often on behalf of the government. Sensitive research, much of which occurs in the unclassified realm, is the key to our nation's global advantage, both economically and militarily.

The Counterintelligence (CI) Domain Program is responsible for determining and safeguarding those technologies which, if compromised, would result in catastrophic losses to national security. Through our partnerships with businesses, academia, and U.S. government agencies, the FBI and its counterintelligence community partners are able to identify and effectively protect projects of great importance to the U.S. government. This provides the first line of defense inside facilities where research and development occurs and where intelligence services are focused.

The following initiatives make up our CI Domain Program:

Business Alliance

Through the Business Alliance, we are building relationships with cleared defense contractors to enhance their understanding of the threat posed to their programs and personnel by foreign intelligence services and foreign competitors. This dialogue results in an increase in the quality and quantity of counterintelligence-related information shared with the FBI by these contractors, resulting in the disruption of foreign intelligence activities targeting their work.

Through the delivery of counterintelligence education and the sharing of actionable intelligence, we enable business partners to identify counterintelligence vulnerabilities within their organizations. Counterintelligence awareness can result in modifications to their internal behaviors and processes that decrease susceptibility to theft of intellectual property. The protection of our Business Alliance partners' intellectual property results in tangible benefits to our

Westpfahl&Spilker

Fallgestaltung 3:

Informationsverschaffung über Mutter-Tochter-Konstellationen

Fallgestaltung 4:

Invasive Maßnahmen

Beispiel: Verhaftung der UBS Mitarbeiter Martin Liechti sowie Bradley Birkenfeld

§ 30 OWiG
Geldbuße gegen juristische Personen und Personenvereinigungen

(1) Hat jemand

1. als vertretungsberechtigtes Organ einer juristischen Person oder als Mitglied eines solchen Organs,

[…]

5. als sonstige Person, die für die Leitung des Betriebs oder Unternehmens einer juristischen Person oder einer in Nummer 2 oder 3 genannten Personenvereinigung verantwortlich handelt, wozu auch die Überwachung der Geschäftsführung oder die sonstige Ausübung von Kontrollbefugnissen in leitender Stellung gehört,

eine Straftat oder Ordnungswidrigkeit begangen, durch die Pflichten, welche die juristische Person oder die Personenvereinigung treffen, verletzt worden sind oder die juristische Person oder die Personenvereinigung bereichert worden ist oder werden sollte, so kann gegen diese eine Geldbuße festgesetzt werden.

[…]

(3) § 17 Abs. 4 und § 18 gelten entsprechend.

§ 17 OWiG
Höhe der Geldbuße

[…]

(4) Die Geldbuße soll den wirtschaftlichen Vorteil, den der Täter aus der Ordnungswidrigkeit gezogen hat, übersteigen. Reicht das gesetzliche Höchstmaß hierzu nicht aus, so kann es überschritten werden.

Urteil des BGH vom 15.11.2001 – Rechtliche Beurteilungen/Objektiver Tatbestand

- Der Tatbestand der Untreue gemäß § 266 StGB wird bejaht.
- Es liegt der Missbrauchstatbestand vor, definiert dahingehend, dass durch das Können im Außenverhältnis das Dürfen im Innenverhältnis überschritten wird.
- Tatbestandserfüllung durch Übernahme unvertretbarer Risiken und damit Verletzung der Vermögensinteressen des Kreditinstituts wird bejaht.
- Verstößen gegen die Anforderungen des § 18 KWG kommt Indizwirkung in Richtung auf pflichtwidriges Handeln im Sinne des § 266 StGB zu.
- Ausdrückliches Abrücken von der Interpretation eines Urteils des gleichen BGH-Senats (vom 06.04.2000, BGHSt 46, 30) durch die Praxis, wonach bei Verletzung des § 18 KWG Rückschlüsse auf das Eingreifen des Untreuetatbestandes unzulässig sein sollten.

- Die diesbezüglich entscheidenden Passagen des Urteils vom 15.11.2001 lauten:

> „Für die Grenzen des rechtlichen Dürfens kommt es allein darauf an, ob die Angeklagten ihrer Prüfungs- und Informationspflicht bezüglich der Vermögensverhältnisse der Kreditnehmer ausreichend nachgekommen sind. Tatsächliche Anhaltspunkte dafür, daß die Risikoprüfung nicht ausreichend vorgenommen wurde, werden sich insbesondere daraus ergeben, daß die Informationspflichten vernachlässigt wurden. Aus der Verletzung der in § 18 Satz 1 KWG normierten Pflicht zum Verlangen nach Offenlegung der wirtschaftlichen Verhältnisse können sich Anhaltspunkte dafür ergeben, daß der banküblichen Informations- und Prüfungspflicht nicht ausreichend Genüge getan wurde. Die Vorschrift dient dem Schutz des einzelnen Kreditinstituts und seiner Einleger. Sie hält Kreditinstitute über die Kreditwürdigkeitsprüfung zu einem risikobewußten Kreditgabeverhalten an. Das hat das Bundesaufsichtsamt für Kreditwesen (BAKred) in seinem Rundschreiben 9/98 vom 07.07.1998 ausführt. § 18 KWG beinhaltet daher eine Selbstverständlichkeit, hebt sie aber zu einer gesetzlichen Norm. Die Verpflichtung des § 18 Satz 1 KWG besteht während der gesamten Dauer des Engagements. Das Kreditinstitut muß die wirtschaftliche Entwicklung des Kreditnehmers während der gesamten Dauer des Kreditverhältnisses kontinuierlich beobachten und analysieren. Die Verlautbarungen des BAKred verdeutlichen, daß § 18 KWG eine zentrale Bestimmung für die Kreditvergabe und die damit verbundene Kreditwürdigkeitsprüfung ist, die nicht nur – formal – sondern materiell einzuhalten ist. Dem gemäß hat der XI. Zivilsenat des BGH ausgesprochen (WM 1994, 838), dass die Kreditinstitute verpflichtet sind, sich nachhaltig um die Vorlage von Jahresabschlüssen beziehungsweise einen Vermögensstatus mit ergänzenden Angaben zu bemühen und die weitere Kreditgewährung von einer solchen Vorlage abhängig zu machen, den Kredit also zu kündigen, wenn ihnen die Erfüllung ihrer gesetzlichen Verpflichtung durch das weitere Verhalten ihres Kunden unmöglich gemacht wird.“

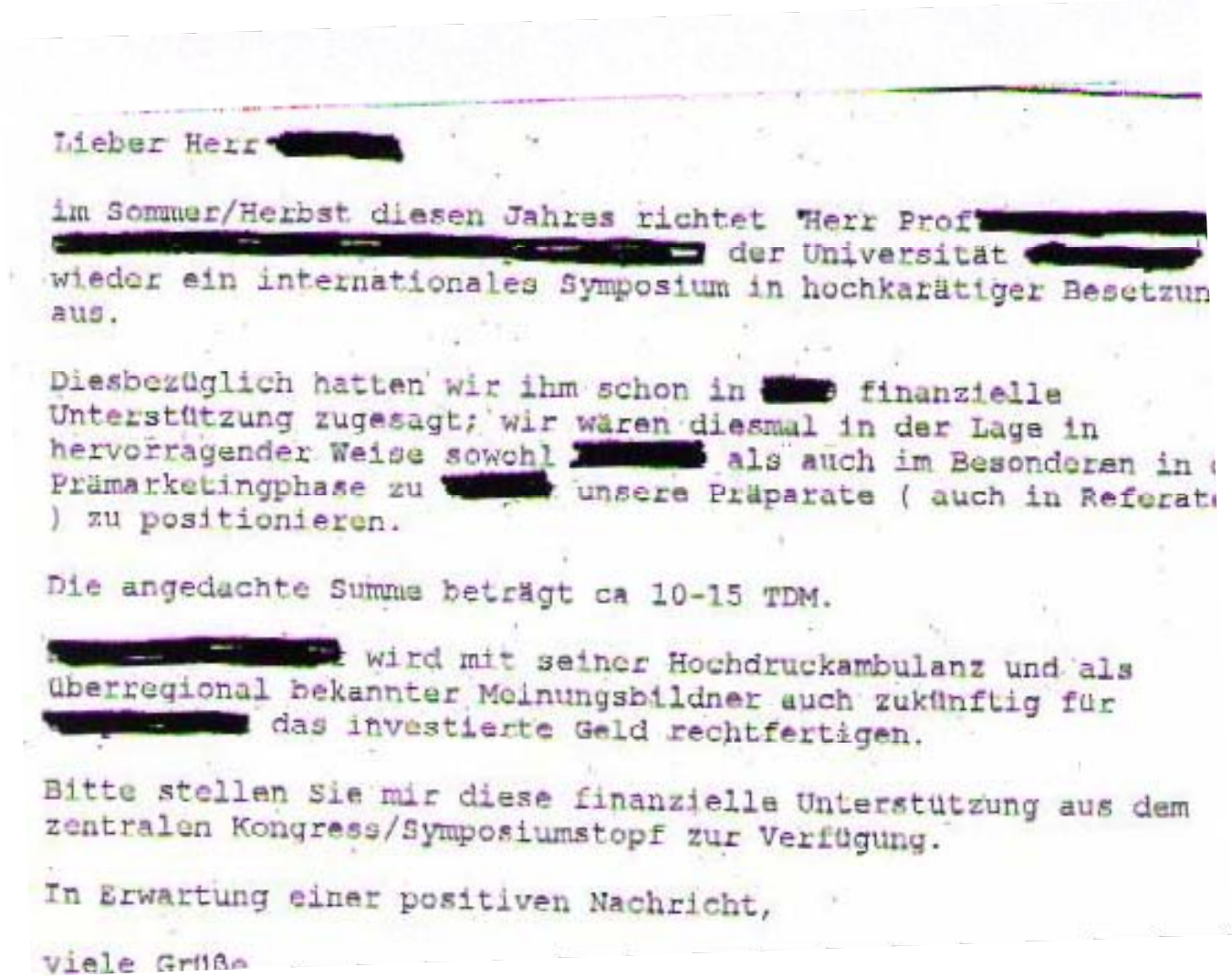
Urteil des BGH vom 15.11.2001 – Rechtliche Beurteilungen/Subjektiver Tatbestand

- Im Falle massiver Verstöße gegen § 18 KWG wird seitens des BGH der Vorsatz bei Verwirklichung des Untreuetatbestandes bejaht.

- Dass für das Kreditinstitut durch den Täter ein Erfolg des Engagements gewünscht wird, steht der Annahme vorsätzlichen Handelns nicht entgegen.

- Die diesbezüglichen Formulierungen des BGH lauten:

  „Allein auf die Vermögensgefährdung muß sich das Wissenselement beziehen (BGH, wistra, 1993, 265; NSTZ 1999, 353). Das Wissenselement des Schädigungsvorsatzes fällt folglich nicht deshalb weg, weil der Bankleiter beabsichtigt, hofft oder glaubt, den endgültigen Schaden abwenden zu können. Erforderlich ist vielmehr nur, daß der Bankleiter zum Zeitpunkt der Kreditgewährung die Minderwertigkeit des Rückzahlungsanspruches im Vergleich zu der ausgereichten Darlehensvaluta gekannt hat. Dazu freilich reicht bereits seine Kenntnis, der die Vermögensgefährdung begründenden Umstände und das Wissen, daß die Forderung nach allgemeinen Bewertungsmaßstäben nicht als gleichwertig angesehen wird, mag er selbst sie auch anders bewerten (BGH, wistra 1993, 263). Dementsprechend muß sich auch das Billigungselement des bedingten Vorsatzes auf die schadensgleiche Vermögensgefährdung beziehen.“



Lieber Herr [redacted]

Im Sommer/Herbst diesen Jahres richtet Herr Prof [redacted] der Universität [redacted] wieder ein internationales Symposium in hochkarätiger Besetzun aus.

Diesbezüglich hatten wir ihm schon in [redacted] finanzielle Unterstützung zugesagt; wir wären diesmal in der Lage in hervorragender Weise sowohl [redacted] als auch im Besonderen in Prämarketingphase zu [redacted] unsere Präparate (auch in Referat) zu positionieren.

Die angedachte Summe beträgt ca 10-15 TDM.

[redacted] wird mit seiner Hochdruckambulanz und als überregional bekannter Meinungsbildner auch zukünftig für [redacted] das investierte Geld rechtfertigen.

Bitte stellen Sie mir diese finanzielle Unterstützung aus dem zentralen Kongress/Symposiumstopf zur Verfügung.

In Erwartung einer positiven Nachricht,

viele Grüße

Westpfahl&Spilker

Text der email eines Rechtsanwalts an einen anderen Rechtsanwalt/ Steuerberater vom 04.01. (sinngemäß):

„Beigefügt erhalten Sie den wunschgemäß rückdatierten Vertrag, der den Stand unserer Verhandlungen per 03.01. beschreibt.“

email-Anfrage eines FBI Mitarbeiters:

- Informationen über abgelehnte Exportanfragen aus dem Iran
- Aktuelle Informationen zu bereits mitgeteilten (abgelehnten) Exportanfragen aus Jordanien/Pakistan
- Bereitschaft zur Teilnahme an „Probekäufen“ und sonstigen, verdeckten Transaktionen (agent provocateur) in diesen Ländern